UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
- v. -	:	
VIRGIL GRIFFITH,	:	20 Cr. 15 (PKC)
Defendant.	:	

GOVERNMENT'S CONSOLIDATED MEMORANDUM OF LAW IN OPPOSITION TO THE DEFENDANT'S MOTIONS FOR A BILL OF PARTICULARS, TO COMPEL DISCOVERY, AND TO DISMISS THE INDICTMENT

AUDREY STRAUSS
Acting United States Attorney for the
Southern District of New York
One St. Andrew's Plaza
New York, New York 10007

Michael K. Krouse
Kimberly J. Ravener
Kyle Wirshba
Assistant United States Attorneys
-Of Counsel-

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases **Page(s)**

Statutes

Rules

Regulations

PRELIMINARY STATEMENT

The Government respectfully submits this consolidated memorandum of law in opposition to three motions filed by the defendant Virgil Griffith: (1) to dismiss the indictment (Dkt. 65 ("Mot. to Dismiss")); (2) for a bill of particulars (Dkt. 62 ("Mot. for Particulars")); and (3) to compel discovery (Dkt. 63 ("Mot. to Compel"), collectively the "Defense Motions").

As explained in detail below, the Court should deny the defendant's motion to dismiss because: (1) the Indictment is facially sufficient; (2) the Government will prove at trial the elements of the offense charged; (3) the defendant's conduct does not fall within the "informational materials" exception to the North Korean Sanctions Regulations; and (4) the charge against the defendant does not violate the defendant's rights under the First and Fifth Amendments to the U.S. Constitution. The Court should also deny the defendant's motion for a bill of particulars, because the Complaint, the Indictment, the discovery productions, and the detailed discussions of the evidence in this brief and the brief in opposition to the defendant's motion to dismiss for lack of venue have provided the defendant with adequate notice of the charges so that he can prepare for trial. Finally, the Court should deny the defendant's motion to compel additional discovery, because: (1) OFAC is not a member of the prosecution team; (2) the defense does not provide a legitimate reason to compel the Government to disclose Witness-2's identity now; and (3) the additional information sought from other governmental agencies is not in the possession of the prosecution team and not material to the defense. Accordingly, the Defense Motions should be denied in their entirety.

BACKGROUND

I. PROCEDURAL HISTORY AND RELEVANT FACTS

On November 21, 2019, Virgil Griffith was charged in a detailed criminal Complaint with conspiring to violate the International Emergency Economic Powers Act ("IEEPA"), 50 U.S.C.

§§ 1701-1706. One week later, Griffith was arrested in Los Angeles pursuant to the charge in the Complaint. On January 7, 2020, a Grand Jury sitting in this District returned an Indictment charging the defendant with one count of conspiring to violate IEEPA by providing prohibited services to the Democratic People's Republic of Korea ("DPRK"). The defendant, a cryptocurrency expert, traveled to the DPRK and provided services in violation of IEEPA by, among other things, serving as a keynote speaker at the "Pyongyang Blockchain and Cryptocurrency Conference" (the "Conference"), during which Griffith advised the approximately 100 North Korean attendees on how blockchain and cryptocurrency technologies could be used to evade sanctions and launder money. Prior to traveling to the DPRK, Griffith requested permission from the U.S. State Department to attend the Conference, but due to the North Korea Sanctions Regulations ("NKSR"), the U.S. State Department denied the request. Ignoring this denial, Griffith obtained a DPRK visa and unlawfully traveled through China to the DPRK.

A. Griffith's Intent to Violate Sanctions

The evidence will establish that Griffith's participation in the Conference was rooted in his intent to evade DPRK sanctions and assist North Koreans in doing the same. Griffith worked for Ethereum Foundation, a company that functions as an open-source platform for the development of cryptocurrency[1] and blockchain[2] technologies, including a cryptocurrency called Ethereum.

[1] As described in the Complaint, cryptocurrency is a decentralized, peer-to-peer form of electronic currency that can be digitally traded and functions as (1) a medium of exchange; (2) a unit of account; and/or (3) a store of value, but does not have legal tender status. Unlike "fiat currency," such as the U.S. dollar and the Euro, cryptocurrency is not issued by any jurisdiction and functions only by agreement within the community of users of that particular currency. *See* Compl. ¶ 12.

[2] As described in the Complaint, a blockchain is a public, distributed electronic ledger that, among other things, records cryptocurrency transfers. The blockchain only records the movement of cryptocurrency; it does not by itself identify the parties to the transfer. As a result, the users can remain anonymous. *See* Compl. ¶ 13.

Griffith began developing plans to evade sanctions through these technologies more than a year before he traveled to the Conference.

For example, as early as on or about February 17, 2018, Griffith attempted to enlist another individual in a scheme to set up unlawful cryptocurrency equipment in the DPRK. He proposed, over an encrypted instant messaging application, "[i]f you find someone [in North Korea], we'd love to make an Ethereum trip to DPRK and setup an Ethereum node."[3] When the individual questioned whether the plan made "economic sense," Griffith responded, "It does actually[.] It'll help them circumvent the current sanctions on them." (USAO_000427).

Griffith also knew that facilitating sanctions evasion, and supplying his own services to help the DPRK do so, was a critical objective of the Conference. For example, on or about August 31, 2018, an individual asked Griffith, via the same encrypted instant messaging application, why he was willing to risk his safety to go to a conference in the DPRK. Griffith expressed that he was unafraid of the DPRK authorities, because "DPRK wouldn't want to scare away Blockchain talent that'll let them get around sanctions." In response, the individual asked, "What if they're funding their drug trade and nuclear program with crypto?" Griffith replied, "Unlikely. But they'd probably like to start doing such." (USAO_000427).

In another conversation discussing the Conference, on or about November 26, 2018, Griffith wrote that the DPRK's interest in cryptocurrency was "probably avoiding sanctions . . . who knows." (*Id.*).

[3] A "node" is a computer that connects to a cryptocurrency network that is responsible for validating and relaying cryptocurrency transactions. Depending on the cryptocurrency and type of node, a computer acting as a node is often rewarded for the validation it undertakes with additional cryptocurrency, in a process called mining. An individual running a node, therefore, might also receive cryptocurrency as part of the process.

B. Griffith's Arrangements to Attend the Conference

Despite his understanding that the DPRK sought to utilize his expertise for sanctions evasion, and potentially to aid drug trafficking and nuclear proliferation, Griffith began preparations to travel to North Korea by early 2019. In order to attend and present at the Conference, Griffith learned he had to obtain the approval of the DPRK Mission in Manhattan. On or about February 14, 2019, Griffith received an email from a co-conspirator ("CC-1"), bearing the subject, "Applying for blockchain conference," and stating, in substance and in part:

> Because you have US passport, I already sent your data to my department in Pyongyang, the Committee for Cultural Relations with Foreign Countries. But they only can give the clearance after the first approval of our DPRK mission in NY. So, please communicate ASAP with: DPRK Mission to the U.N. E-mail: dpr.korea@verizon.net . . . Address: 820 Second Avenue, 13th Floor New York, NY 10017 USA[.] You have have [sic] to express your wish to participate in the blockchain conference from 18 to 25 April 2019, invited by the Committee for Cultural Relations with Foreign Countries. You can give the Reference/Contact person in Pyongyang: Mr. Kim Won Il, Committee for Cultural Relations with Foreign Countries. You also have to send them your passport, personal details and CV (Resume).

(USAO_004274). In response to the email from CC-1 and consistent with CC-1's instructions, Griffith sent an email to "dpr.korea@verizon.net" on or about February 18, 2019, which included the following:

> Hello to UN's DPRK Mission. I'm writing to you to request your permission to attend and speak at the blockchain conference from 18 to 25 April 2019. I have been invited by the Committee for Cultural Relations with Foreign Countries. My contact person in Pyongyang is: Mr. Kim Won Il, Committee for Cultural Relations with Foreign Countries. I attach my passport, and CV.

(*Id.*).

The email address provided by CC-1, however, was incorrect; as reflected in publicly available materials, the DPRK Mission in Manhattan uses "DPRK.UN@verizon.net" as its email address. On or about March 7, 2019, Griffith forwarded his prior email to the correct email address, writing: "This is my request to visit the DPRK blockchain conference. See forwarded

email below." Griffith also attached a picture of his passport and a digital link to his curriculum vitae, as CC-1 directed would be necessary to procure "the first approval of our DPRK mission in NY." (*Id.*).

On or about April 17, 2019, approximately one month after contacting the DPRK mission in New York, Griffith received a visa to visit the DPRK, a copy of which he later posted to his Twitter account. Griffith admitted to law enforcement that he kept his visa separate from his passport in order to hide his travel to the DPRK from U.S. authorities. (USAO_001558).

C. Griffith's Attendance and Presentation at the Conference

Griffith flew to the DPRK on April 18, 2019. The Conference occurred on April 23 and 24. Griffith departed the DPRK on April 25.

At the Conference, in violation of the NKSR, Griffith provided services to the DPRK attendees to facilitate sanctions evasion by: giving a presentation on topics that had been pre-approved by DPRK officials, including cryptocurrency and blockchain technologies; supplying the conference attendees and participants with information on blockchain and cryptocurrency technologies and their applications; answering questions about these technologies from conference attendees and participants; and participating in discussions regarding the potential uses for blockchain and cryptocurrency technologies to evade sanctions and launder money. Griffith was assigned a DPRK-government handler throughout his trip to North Korea, and at times, wore a North Korean military-style uniform.

During the course of the investigation, the Government has obtained, and produced to the defense in discovery, audio recordings from the Conference. The Government has also recovered from the defendant's electronic devices and accounts video clips of the Conference and the defendant's remarks, as well as notes written by Griffith for his presentation. One of the audio recordings captured the following statements made at the Conference by Griffith:

> Hi everyone. My name is Virgil. I work for a group called the Ethereum Foundation. We do a sort of, next generation blockchain. I think the most valuable things we have to offer the DPRK are number one—we can give you, so blockchain gives you payments that the USA can't stop. And number two—we can give you contracts that don't go through the UN. So, if you make a contract with someone and the U.S. decides "oh, we don't want to do that anymore," you can still hold them to it. And that's kind of the two new things. Like before, if you send payments, you had to I guess, go through the U.S., and for international agreements, you had to go through the UN. With this new technology, you don't have to do that anymore and it's like, you know, great.
>
> I suppose like one, not so good thing about this, is that the technology is still fairly new—maybe ten years told. So we haven't really, we don't really, like no one knows how to do all this right yet, but we definitely think this will be really useful for the DPRK, and that's why we're here. And if the DPRK adopts this, they will be on the very leading edge of technology.

(USAO_002621- USAO_002622). During the same part of the Conference, one of the defendant's other co-conspirators ("CC-2") made the following statements,[4] in the defendant's presence, to the Conference audience:

> So I'm going to outline now a way in which countries like Iran are now using blockchain in order to get around these sanctions that were placed on their banks.
>
> . . .
>
> So in summary, the blockchain for moving money around the world is not only very, very easy, especially for a county like the DPRK which has been imposed with the most horrific sanctions by the US government, but also it's quicker, faster, more safe, and easier.

(USAO_002623, USAO_002625).

Another recording captured what the Government understands to be a portion of Griffith's presentation at the Conference, during which he made the following statements, in substance and in part:

[4] Before trial, the Government intends to file a motion *in limine* that will seek to admit the statements of CC-1 and CC-2 against the defendant at trial, pursuant to Federal Rules of Evidence 801 and 804.

> Hello everyone, I know it's late in the day so I'll try to make this fun. So the most important feature of blockchains is that they are open. *And the DPRK can't be kept out no matter what the USA or the UN says*.
>
> . . .
>
> One of the more interesting things is that blockchains allow greater self-reliance in both banking and contracts. So you can have contracts without an authority. . . . *So you've heard about with blockchain the USA can't stop your payments. So that's like step 1; step 2 is that the UN can't stop agreements. So if DPRK makes agreements with someone, or if an individual does, it's, you can, you don't have to go to a court.*
>
> . . .
>
> "[T]hat would suggest that if the DPRK wanted to explore this, would be to set up a small research group to study what kinds of contracts they would like to have all over the world that could be enforced on blockchain, not all of them can. But this is an active research area in science, actually no one really knows how to do this well yet, but y'all could be the first.

(USAO_002639, USAO_002641 (emphasis added)). These remarks were consistent with Griffith's notes, which were recovered from a laptop that Griffith took with him to the DPRK. Those notes stated, in part, "Blockchains are open—DPRK can't be kept out," "[t]he USA won't be able to stop payments," and "[t]he UN won't be able to stop or cancel agreements." (USAO_001647). The notes also included a "to do" list, which included "[a]ttempt to acquire" two DPRK-based internet domains relating to cryptocurrency—blockchain.kp, and crypto.kp. (*Id*.)

After Griffith's presentation, Griffith and CC-2 answered questions from North Korean Conference attendees with the assistance of an interpreter, which focused on the technical aspects of blockchain and cryptocurrencies, and on the way in which those technologies could be used to evade sanctions. For instance, one North Korean attendee asked whether the regulation of blockchain and cryptocurrencies would be expected to increase over time. CC-2 responded:

> The issue with blockchain technology is let's say, a regulator does regulate against something or a government, let's say the US tomorrow says all transactions on cryptocurrency between the DPRK and the rest of the world are banned, the question becomes: how can they ban it? The answer is they can't, because unless they were to gather every single computer on the entire planet, and program each and every single one of these computers that they would not be able to accept cryptocurrency transactions from DPRK, which is impossible, no one could ever do that, then it will always work. As long as there is an internet connection that the DPRK has, and someone on the other side has, then the transaction can happen. So it is more or less impossible, even if they were to create a law, or to create a sanction, that that sanction would be enforced. They couldn't enforce that sanction. Not like the current system where they just send a letter or maybe Swift and say don't process the transaction. You can't do that with a blockchain because it's hundreds of thousands of millions of individual computers owned by individual people that would be making that transaction happen.

(USAO_002644).

The same questioner then appears to have asked a follow-up question about whether the DPRK could access the exchanges where cryptocurrencies are traded, or whether they had to use "OTC [*i.e.* over the counter] service providers," which could be difficult due to U.S. sanctions. In response, CC-2 and Griffith made the following statements:

> **CC-2:** That's a really good question.
>
> **Griffith:** I like him, he's really smart.
>
> **CC-2:** So let me explain to you, so in essence not much difference. The difference between an OTC provider and an exchange is an OTC means that the purchasing is happening off the market. What that means is that, the rest of the market can't see that you bought that bitcoin. So it's as if, with Dr. Virgil, he decided to privately sell me his bitcoin, or his USDT, but we do it agreed between ourselves, we don't agree it and then everyone in the room knows we did it. We go outside and we have a conversation and we sent it between ourselves. So that tends to be a way in which governments and large entities prefer to do the transaction because don't want the whole world knowing that they just moved a significant amount of money between each other.
>
> In terms of your question on sanctions, the largest OTC desks in the cryptocurrency space, most of them operate out of China. So most of them, the DPRK obviously has more friendly relations with China than probably any of the other large powers at this current stage, and I personally don't think that finding an OTC provider in China would be very difficult for DPRK.

. . .

Griffith: And if China doesn't work, Singapore will probably be able to do it.

(USAO_002644- USAO_002645).

During another part of the Conference, a Conference attendee asked, in Korean, for a "more clear idea of what is blockchain." Griffith responded:

> So I was asked what a blockchain is, and so there are several ways of looking at it. The most abstract one is that it is a database where no single person has a back end access where they can get in. So before when there were different data bases . . . it lives on one server somewhere. Where that server is . . . the government could edit . . . and control it. Blockchain is interesting in that the database is split among servers all over the world. So this makes the data base slower but it makes it where no single person can control it. That's fundamentally the new idea.
>
> The new idea's having a database that we can all read from and we can all pay a very small amount of money in order to write to it. And anyone can do this.
>
> So the term blockchain—so a block, basically it is a list of updates. Let's say a sends money to B or something like that so this whole block is like a list of a hundred transactions and the chain tells you which order the transaction goes through. So if you have two transaction—say A sends money to B, or A sends money to C, you have to know which ones came first. So the block says what are the transactions and the chain says what order they go in.
>
> Probably the coolest thing about blockchain is that it lets you treat digital data in a new way. So before, let's say you have a movie, you can always copy the movie and give it to your friends. This is not very good for money—you can't really copy money, that doesn't really work anymore. Blockchain is the ability that when you give . . . to someone, you can no longer give it to someone else.

(USAO_002658- USAO_002659). The Government also intends to offer at trial a video clip of the defendant providing the first paragraph of the remarks above.

Finally, during another part of the Conference, Griffith made the following statements, in substance and in part:

> So, a lot of this technology is still very new and most of this paper is about different tradeoffs and you know, how to make it resistant to different kinds of attacks. So if like the U.S. wanted to corrupt the blockchain, what are some ways to make it harder for them to do it? People haven't really decided that's like the best design

> yet, but the designs are getting better and, yeah, so I guess, starting now would be a way to get in early and achieve dominance.

(USAO_002661).

A Conference attendee then asked whether exists "any organization or party that manages or takes charge of [Bitcoin's] distributive database system." Griffith responded:

> Yeah, that's an easy question with a hard answer. So there is a group that does upgrades to Bitcoin. But they don't try to control it. So one of the interesting things about blockchain is that if you don't like how it's being run, you can always copy it and make your own. So there is a current group that does this—they're called Bitcoin Core, and—but you know, they're not part of the U.S. They're just random people all over the world. If you decide that you don't like them, you can just go without them and there's no problem. So in short, there is a group, they do upgrades, but you aren't tied to them—you can go without them if you want.

(USAO_002661, USAO_002663).

D. Griffith's Statements to the FBI After the Conference

After the Conference, FBI agents interviewed Griffith in person on May 22, 2019 (USAO_000001-USAO_000007), and November 12, 2019 (USAO_000242-000252). The FBI also interviewed Griffith over the phone on November 6, 2019 (USAO_000233-000237).

During these interviews, Griffith acknowledged that he traveled to the DPRK to attend the Conference as the keynote speaker. He acknowledged that he knew it was illegal for U.S. citizens to travel to the DPRK, and that the State Department denied his request for permission to travel to the DPRK. Griffith told the agents that he had corresponded with officials at the DPRK Mission in Manhattan to facilitate his travel, and that he had sent the requested documents for travel to the DPRK's Mission email address. Griffith also stated that he paid the Conference organizer 3,000 to 3,500 Euros to attend the Conference, and that he believed some of that money might have been provided to the DPRK's government.

Griffith stated that, prior to the Conference, he received approximately 15 PDF files of technical papers, which CC-2 had provided to the DPRK government, and which the DPRK

government had approved for the Conference. CC-2 told Griffith to create his presentation for the conference using this "approved content." According to Griffith, CC-2 told Griffith to stress in his remarks that cryptocurrency and blockchain technologies could be used for "money laundering" and "sanctions evasion," since that was the basis for the attendees' interest in those technologies. In preparation for his remarks, Griffith developed a PowerPoint presentation that was based on these approved PDFs.

Griffith also described the Conference to agents. Griffith stated that the Conference had approximately 100 attendees, only some of whom appeared to understand cryptocurrency and blockchain technology. Griffith also described three young males who sat in the back and asked more technical and specific questions, including questions that addressed complex topics, such as "proof of work" versus "proof of stake" in the mining of cryptocurrencies. As to Griffith's keynote address, Griffith reported that there were technical difficulties, so Griffith discussed the topics in his PowerPoint presentation verbally and used a whiteboard to draw diagrams during his discussion.

Griffith acknowledged to the agents that the PDFs were like a course textbook, and that Griffith was the lecturer who explained the content to the audience like a teacher. He assessed that he may have introduced new concepts to the North Korean Conference attendees, and that the attendees left with a better understanding of blockchain and cryptocurrency technologies. Griffith also noted that a major selling point to the North Koreans at the conference was that cryptocurrency could make the DPRK independent from the international banking system.

At the first interview, on May 22, 2019, Griffith informed the agents of his desire to return to the DPRK, and to facilitate cryptocurrency exchanges with the DPRK. The agents advised Griffith that doing so would likely violate U.S. law, to include the prohibitions associated with

IEEPA. However, even after this admonishment, the defendant continued to contemplate providing additional services to the DPRK. For instance, on or about August 6, 2019, Griffith wrote to another person ("Individual-1"):

Griffith: I want to go back to North Korea.

. . .

Individual-1: Why? What do you hope to gain from your second visit?

Griffith: I need to send 1 [unit of Ethereum] between North and South Korea.

Individual-1: Isn't that violating sanctions?

Griffith: It is. That's why I'm going to get a South Korean to do it.

. . .

Individual-1: What [South Korean] would dare to take that risk?

Griffith: I'd do it

Individual-1: You aren't South Korean.

Griffith: Just need to find a South Korean Virgil.

Individual-1: oh lol

Griffith: There's got to be at least one who wants to make a name . . .

Individual-1: Would it damage the reputation of Ethereum?

Griffith: I predict it will be a net positive

Individual-1: It makes me nervous for you to defy the US government and go again

Griffith: I'll figure something out . . . Worst comes to worst I'll send an emissary.

(USAO_000427).

The next day, on August 7, 2019, Griffith sent an audio recording to Individual-1, in which Griffith stated: "Probably worst comes to worst, I'll find someone to send as like an emissary to

go and I'll like tell that person what to do via the phone. Yeah, I can always do that, because it seems like the Americans let you get away with it once." (*Id.*).

II. DISCOVERY PRODUCTIONS

Since the defendant's indictment, the Government has produced extensive discovery to the defense. Specifically, between January 23, 2020 and October 27, 2020, the Government made 13 discovery productions. The initial discovery production included reports containing the defendant's statements to the FBI, the defendant's cellphone extraction, and search warrants and associated applications for Griffith's cellphone and its geolocation, two of Griffith's email addresses, his iCloud account, and his social media accounts. Subsequent productions included, among other things, audio recordings from the Conference, search warrants and associated affidavits for Griffith's luggage, Singaporean laptop, and two email accounts belonging to co-conspirators, returns from each of these search warrants, as well as extractions from electronic devices, including cellphones, tablets, and computers. Moreover, in August 2020, the Government obtained and produced, in response to a defense request, internal U.S. State Department communications, as well as communications that the prosecution team had with the Treasury Department's Office of Foreign Asset Control ("OFAC"). At the defense's request, the Government also asked for OFAC's internal communications, which OFAC declined to produce.[5] The Government also produced, at the defendant's request, all of its communications with law

[5] In a footnote, the defendant asserts that the Government's request to OFAC for materials at the request of the defendant was a "tacit recognition of the relevance of these materials." (Mot. to Compel 8 n.6). The Government, however, has taken no position on the relevance of whatever information OFAC has declined to produce, and was simply seeking to accommodate a defense request as a courtesy. As explained *infra*, these OFAC materials lie outside the possession of the prosecution team, and the prosecution team has not seen whatever materials may or may not exist within OFAC.

enforcement authorities in Singapore, as well as reports describing the FBI's evaluation of intelligence derived from its investigation of Griffith and his co-conspirators.

The Government has also provided the defense with materials that are not subject to Rule 16 but may ultimately be subject to 18 U.S.C. § 3500. Specifically, between July and October 2020, the Government produced reports, notes memorializing statements, and email communications from 10 different witnesses.

DISCUSSION

I. THE MOTION TO DISMISS THE INDICTMENT SHOULD BE DENIED

The defendant asserts that the Court should dismiss the Indictment for two reasons. First, the defendant claims that the Indictment does not provide adequate notice of the offense charged, as required by the Fifth and Sixth Amendments to the U.S. Constitution. (Mot. to Dismiss at 9-10). Second, the defendant asserts that the Indictment fails to state a criminal offense. (Mot. to Dismiss at 10-25). Because the Indictment is facially sufficient, the Court should deny the defendant's motion in its entirety. Even if the Court were to look beyond the Indictment, however, the anticipated trial evidence is sufficient to establish a conspiracy to violate IEEPA by providing services to the DPRK. For all of these reasons, the defendant's motion to dismiss is meritless and should be denied.

A. Applicable Law

1. IEEPA

IEEPA authorizes the President "to deal with unusual and extraordinary threat[s] . . . to the national security, foreign policy, or economy of the United States" by declaring a national emergency with respect to such threats, and to take steps to address such threats. 50 U.S.C. § 1701(a). Criminal penalties under IEEPA are reserved for those who "willfully commit[], willfully attempt[ ] to commit, or willfully conspire[ ] to commit" a violation of any license, order

or regulation issued pursuant to IEEPA. *Id.* § 1705(c). IEEPA exempts those who act in "good faith" reliance on IEEPA, or on "any regulation, instruction, or direction" issued under IEEPA, from both civil and criminal liability. *Id.* § 1702(a)(3).

Beginning with Executive Order 13466, issued on June 26, 2008, the President found that the situation "on the Korean Peninsula constitute[s] an unusual and extraordinary threat to the national security and foreign policy of the United States and . . . declare[d] a national emergency to deal with that threat." (Exec. Order 13466). Following the issuance of Executive Order 13466, OFAC promulgated the North Korea Sanctions Regulations ("NKSR") to implement sanctions on the DPRK. *See* 31 C.F.R. Part 510.

On August 30, 2010, the President "expand[ed] the scope of the national emergency declared in Executive Order 13466" finding that

> the continued actions and policies of the Government of North Korea, manifested most recently by its unprovoked attack that resulted in the sinking of the Republic of Korea Navy ship Cheonan and the deaths of 46 sailors in March 2010; its announced test of a nuclear device and its missile launches in 2009; its . . . procurement of luxury goods; and its illicit and deceptive activities in international markets through which it obtains financial and other support, including money laundering, the counterfeiting of goods and currency, bulk cash smuggling, and narcotics trafficking, destabilize the Korean peninsula and imperil U.S. Armed Forces, allies, and trading partners in the region, and thereby constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States.

(Exec. Order 13551). In light of these harms, the President authorized the sanctioning of additional individuals who, for example, "directly or indirectly, engaged in money laundering, the counterfeiting of goods or currency, bulk cash smuggling, narcotics trafficking, or other illicit economic activity that involves or supports the Government of North Korea or any senior official thereof." (*Id.*). The President again authorized additional sanctions on January 2, 2015, citing the DPRK's "destructive, coercive cyber-related actions . . . and commission of serious human rights

abuses [that] constitute a continuing threat to the national security, foreign policy, and economy of the United States." (Exec. Order 13687).

On March 18, 2016, the President issued Executive Order 13722, which imposed comprehensive sanctions on North Korea. It stated that "the Government of North Korea's continuing pursuit of its nuclear and missile programs, as evidenced most recently by its February 7, 2016, launch using ballistic missile technology and its January 6, 2016, nuclear test . . . increasingly imperils the United States and its allies." (Exec. Order No. 13722). Accordingly, the Executive Order imposed an embargo, which prohibited "the exportation or reexportation, direct or indirect, from the United States, or by a United States person, wherever located, of any goods, services, or technology to North Korea" and "any approval, financing, facilitation, or guarantee by a United States person, wherever located, of a transaction by a foreign person where the transaction by that foreign person would be prohibited by this section if performed by a United States person or within the United States." (*Id.*).

Pursuant to Executive Order 13722, and to incorporate certain other legislation, OFAC amended and reissued the NKSR on March 5, 2018. At all times relevant to this case, the NKSR prohibited, among other things, the "exportation or reexportation, directly or indirectly, from the United States, or by a U.S. person, wherever located, of any goods, services, or technology to North Korea" and "[a]ny conspiracy formed to violate the prohibitions set forth in this part." 31 C.F.R. §§ 510.206(a), 510.212(a)-(b).

OFAC's regulations further state that the "prohibition on the exportation and reexportation of goods, services, or technology . . . applies to services performed on behalf of a person in North Korea or the Government of North Korea or where the benefit of such service is otherwise received in North Korea, if such services are performed . . . by a U.S. person." 31 C.F.R. § 510.405(a).

The regulations also state that "U.S. persons may not, except as authorized by or pursuant to this part, provide legal, accounting, financial, brokering, freight forwarding, transportation, public relations, or *other services* to any person in North Korea or to the Government of North Korea." *Id*. § 510.405(d)(1) (emphasis added). The defense does not dispute that Griffith is a U.S. person under these regulations.

2. Motions to Dismiss

"A criminal defendant is entitled to an indictment that states the essential elements of the charge against him." *United States v. Pirro*, 212 F.3d 86, 91 (2d Cir. 2000) (citing *Jones v. United States*, 526 U.S. 227, 232 (1999)); *Hamling v. United States*, 418 U.S. 87, 117 (1974); Fed. R. Crim. P. 7(c)). "A defendant faces a 'high standard' in seeking to dismiss an indictment." *United States v. Thompson*, 2013 WL 6246489, at *6 (S.D.N.Y. 2013) (quoting *United States v. Post*, 2013 WL 2934229, at *5 (S.D.N.Y. 2013)). "[A]n indictment is sufficient if it, first, contains the elements of the offense charged and fairly informs a defendant of the charge against which he must defend, and, second, enables him to plead an acquittal or conviction in bar of future prosecutions for the same offense." *Hamling*, 418 U.S. at 117. "An indictment must be read to include facts which are necessarily implied by the specific allegations made." *United States v. LaSpina*, 299 F.3d 165, 177 (2d Cir. 2002) (internal quotation marks omitted) (citation omitted).

"[T]he sufficiency of the evidence is not appropriately addressed on a pretrial motion to dismiss an indictment." *United States v. Alfonso*, 143 F.3d 772, 777 (2d Cir. 1998). Accordingly, "[i]n reviewing a motion to dismiss an indictment, the Court must take the allegations of the indictment as true." *United States v. Skelos*, 2015 WL 6159326, at *2 (S.D.N.Y. 2015) (citing *Boyce Motor Lines v. United States*, 342 U.S. 337, 343 n.16 (1952); *New York v. Tanella*, 374 F.3d 141, 148 (2d Cir. 2004)).

In the context of conspiracy allegations, "the defendant does not 'need' detailed evidence about the conspiracy in order to prepare for trial properly." *United States v. Feola*, 651 F. Supp. 1068, 1132 (S.D.N.Y. 1987), *aff'd*, 875 F.2d 857 (2d Cir. 1989). Specifically, "defendants need not know the means by which it is claimed they performed acts in furtherance of the conspiracy nor the evidence which the Government intends to adduce to prove their criminal acts." *Id*. Thus, as the Second Circuit has stated, "[t]he Government need not, when charging conspiracy, set out with precision each and every act committed by the conspirators in the furtherance of the conspiracy . . . ." *United States v. Cohen*, 518 F.2d 727, 733 (2d Cir. 1975) (citations omitted); *see also United States v. Trippe*, 171 F. Supp. 2d 230, 240 (S.D.N.Y. 2001) ("[D]emands for particular information with respect to where, when, and with whom the Government will charge the defendant with conspiring are routinely denied.").

B. The Indictment Sufficiently Alleges a Conspiracy to Violate IEEPA

The Indictment is sufficient on its face and should not be dismissed. (*See* Dkt. 53, Opinion and Order at 5-6 (denying defendant's prior motion to dismiss as to venue where "the facial sufficiency of the indictment's allegation" is "enough to survive the defendant's motion")). The sole count of the Indictment properly alleges the essential elements of the crime charged, tracking the language of the relevant statute and specifying the nature, time, and place of the alleged offense.

The Indictment states that, between in or about August 2018 and in or about November 2019, the defendant conspired with others to willfully violate IEEPA, and that he did so in the Southern District of New York, the DPRK, and elsewhere outside of the jurisdiction of any particular State or district of the United States. The Indictment also alleges that the conspiracy included two objects: (1) to provide and cause others to provide services to the DPRK without obtaining approval from OFAC; and (2) to evade and avoid, and to attempt to evade and avoid,

the sanctions against the DPRK by providing services to the DPRK. Finally, the Indictment alleges that these objects of the conspiracy violated 50 U.S.C. § 1705(a), 31 C.F.R. §§ 510.206(a), 510.212(a)-(b), and Executive Orders 13466 and 13722.

Because the Indictment tracks the statutory language, and alleges the period and location of the offense charged, it sufficiently alleges an IEEPA conspiracy. *See United States v. Stavroulakis*, 952 F.2d 686, 693 (2d Cir. 1992) ("We have often stated that 'an indictment need do little more than to track the language of the statute charged and state the time and place (in approximate terms) of the alleged crime.'" (quoting *United States v. Tramunti*, 513 F.2d 1087, 1113 (2d Cir. 1975), *cert. denied*, 423 U.S. 832 (1975))). The Indictment need not, as the defendant contends (Mot. to Dismiss at 9), name or state the identities of the defendant's co-conspirators or describe the evidence that the Government intends to introduce against the defendant at trial. *See Cohen*, 518 F.2d at 733 ("The Government need not, when charging conspiracy, set out with precision each and every act committed by the conspirators in the furtherance of the conspiracy . . . ."); *United States v. Gonzalez*, 2004 WL 2297341, at *1-2 (S.D.N.Y. 2004). Because the Indictment in this case is sufficient under longstanding federal precedent, the defendant's motion to dismiss for lack of specificity should be denied.

C. Griffith's Conduct Constitutes the Provision of Services under IEEPA

Even if the Court was to go beyond the face of the Indictment, the Court should deny the defendant's motion to dismiss because the evidence will establish that the defendant conspired with others to: (1) provide "services" to the DPRK without obtaining approval from OFAC; and (2) to evade and avoid, and to attempt to evade and avoid, the sanctions against the DPRK.

The NKSR does not expressly define the term "service." In the context of analogous sanctions against Iran, however, the Second Circuit has explained that courts should define the term by looking to the "plain and unambiguous meaning with regard to the particular dispute,"

aided by the "broader text and purpose" of the sanctions regime. *United States v. Banki*, 685 F.3d 99, 107 (2d Cir. 2012), *as amended* (Feb. 22, 2012) (internal quotation marks omitted) (citation omitted).

In *Banki*, the defendant was charged with, among other things, conspiring to violate sanctions against Iran by executing money transfers to Iran. *Id*. at 105. On appeal, the defendant argued that the district court erred in failing to instruct the jury that these transfers would only constitute a "service" within the meaning of the sanctions regulations if they were performed for a fee. The Second Circuit rejected this argument. *Id*. at 106; *see also Holder v. Humanitarian Law Project*, 561 U.S. 1, 23–24 (2010) (defining "service," consistent with *Banki*, to mean "the performance of work commanded *or* paid for by another" or "an act done for the benefit or at the command of another") (emphasis added).

The Court looked to the dictionary definitions of "service," observing that at least one dictionary definition included a "fee component," but that many others did not. *Banki*, 685 F.3d at 107. Next, the Court looked "to the broader text and purpose" of the Iranian sanctions regime. *Id.* (citing *United States v. Pesaturo*, 476 F.3d 60, 68 (1st Cir. 2007)). As the Court explained, the "Iranian embargo is intended 'to deal with the unusual and extraordinary threat to the national security, foreign policy, and economy of the United States' posed by 'the actions and policies of the Government of Iran.'" *Id.* at 108 (quoting Exec. Order No. 12,959 and Exec. Order No. 12,957). Moreover, "the embargo is deliberately overinclusive." *Id.* "[T]o reform the actions of the government of Iran, Executive Order 12,959 and the [Iranian sanctions regulations] adopt a blunt instrument: broad economic sanctions intended to isolate Iran." *Id.* (citing *United States v. Homa Int'l Trading Corp.*, 387 F.3d 144, 146 (2d Cir. 2004)). Based on this broader text and

purpose, the Court concluded that the "transfer of funds on behalf of another constitutes a 'service' even if not performed for a fee." *Id.*

The same reasoning applies here. The NKSR is just as comprehensive as the Iranian sanctions at issue in *Banki*. It prohibits not only the exportation or re-exportation of "goods, services, and technology" to anyone inside the DPRK, 31 C.F.R. § 510.206, but also the registering of any vessels in North Korea, *id*. § 510.207, and a prohibition on planes landing in the United States within 180 days of landing in North Korea, *id*. § 510.208. The NKSR permits individual sanctions against those who imported into North Korea "arms" or "luxury goods" and those who "engaged in money laundering, the counterfeiting of goods or currency, bulk cash smuggling, narcotics trafficking, or other illicit economic activity that involves or supports the Government of North Korea or any senior official thereof." *Id*. § 510.201. Indeed, the NKSR even prohibits charitable contributions "of funds, goods, services, or technology, including contributions to relieve human suffering, such as food, clothing, or medicine, . . . by, to, or for the benefit of, or received from, the Government of North Korea, the Workers' Party of Korea, or any other [sanctioned] person." *Id* § 510.408. Just as with the Iranian sanctions, the breadth of these prohibitions illustrate that the purpose of the NKSR is to isolate the DPRK, and to address the "unusual and extraordinary threat to the national security and foreign policy of the United States" that the DPRK represents. (Exec. Order No. 13466; Exec. Order No. 13722). The prohibition on "services" should be read, therefore, sufficiently broadly to effectuate the "broad economic sanctions intended to isolate" North Korea. *Banki*, 685 F.3d at 108.

As explained above, the evidence at trial will establish that the defendant conspired to violate, and to evade and avoid, the DPRK sanctions by, among other things, delivering a keynote address at the Conference, during which the defendant advised the North Korean attendees on how

to evade and avoid sanctions by using blockchain and cryptocurrency technologies. Based on the NKSR's broader purpose, Griffith's presentation constituted a service within the meaning of the NKSR. Even if the information that Griffith presented could be found on the Internet, or distributed in PDF form, Griffith provided a service by synthesizing and explaining this complex information in a way that was accessible to the Conference attendees, and then answering follow-up questions. Delivering this keynote address and answering questions plainly constituted an "act done for the benefit . . . of another." *Humanitarian Law Project*, 561 U.S. at 23–24 (quoting Webster's Third New International Dictionary 2075 (1993)).

Moreover, Griffith described his trip to the DPRK to the FBI in terms consistent with the provision of services under the NKSR. In his interviews with the FBI, Griffith explained that he based his remarks on technical PDFs that he received before the Conference, approved by the DPRK for the Conference, and that his role was to explain this content to the attendees like a teacher. Griffith acknowledged that he may have introduced concepts to the North Korean Conference attendees, and that the attendees likely left the Conference with a better understanding of blockchain and cryptocurrency technologies. The recordings of the Conference further corroborate that Griffith's presentation included explanations of how this technology could be used to evade and avoid U.S. and U.N. sanctions.

The defendant nonetheless asserts that his presentation at the Conference did not constitute a "service" for three reasons. *First*, the defendant asserts that his presentation at the Conference only contained "general" information widely available on the Internet. *Second*, the defendant asserts that he did not receive a fee from the DPRK for his participation in the Conference. *Third*, the defendant asserts that his presentation had no "economic utility." These arguments are unavailing.

Griffith's first argument—that his presentation was "general" and imparted only information widely available on the Internet (Mot. to Dismiss at 12)—is both inaccurate and not a basis for dismissal. As the evidence summarized above establishes, Griffith's remarks were highly targeted and specific regarding the DPRK's desire to use blockchain and cryptocurrencies to evade and avoid U.S. sanctions. Griffith told FBI that, prior to Griffith's keynote, CC-2 instructed him to tailor his presentation to applications of cryptocurrency and blockchain technologies that could be used for "money laundering" and "sanctions evasion." The recordings of Griffith's presentation at the Conference show that Griffith complied with this guidance. (*See* USAO_002621 (stating that blockchain can give the DPRK the ability to make payments "that the USA can't stop"); USAO_002639 ("So the most important feature of Blockchains is that they are open. And the DPRK can't be kept out no matter what the U.S. or UN says."). Far from providing generic information, Griffith's presentation provided the Conference's North Korean attendees with information on technologies that Griffith knew would be used to help the DPRK and its citizens evade U.S. sanctions. Griffith conspired to willfully and intentionally provide this service to the DPRK and its citizens.

Moreover, portions of Griffith's keynote presentation also flatly contradict his self-serving claim that the information he provided to the DPRK was general and widely known. As Griffith explained to the Conference attendees, these technologies are "still fairly new—maybe ten years told," so "no one knows how to do all this right yet, but we definitely think this will be really useful for the DPRK, and that's why we're here. . . . if the DPRK adopts this, *they will be on the very leading edge of technology*." (USAO_002622 (emphasis added); *see also* USAO_002641 ("[T]his is an active research area in science, actually no one really knows how to do this well yet, but y'all could be the first."); USAO_002659 ("Probably the coolest thing about blockchain is

that it lets you treat digital data in a new way."); USAO_002661 ("So if like the U.S. wanted to corrupt the blockchain, what are some ways to make it harder for them to do it? People haven't really decided that's like the best design yet, but the designs are getting better and, yeah, *so I guess, starting now would be a way to get in early and achieve dominance*.") (emphasis added)).

Even if it was true that this information was generic and available elsewhere, the defendant provides no legal basis to interpret "service" as being limited to advice or information that could have only come from Griffith. At the least, Griffith attempted to provide a service in furtherance of the charged conspiracy by synthesizing this technical information, presenting it in an accessible and clear manner to an audience of North Koreans, and answering follow-up questions. A university student could read a book on blockchain, but a professor who provides that student with a lecture on the topic and an opportunity to ask follow-up questions has plainly provided that student with a service.

Griffith next argues that his presentation did not constitute a service because Griffith did not receive a fee. (Mot. to Dismiss at 15 ("Even if a fee is not a dispositive requirement, it nevertheless is a critical factor in determining whether conduct constitutes a 'service' under the applicable regulations."). As explained above, the Second Circuit rejected a similar argument in *Banki*. *See* 685 F.3d at 108 ("[W]e conclude that the execution of money transfers from the United States to Iran on behalf of another, whether or not performed for a fee, constitutes the exportation of a service."). As the court there explained:

> [T]here is no sound reason for the [Iranian sanctions] to distinguish between (1) the exportation of a service to Iran for which the U.S. service provider *received a fee* and (2) the exportation of a service to Iran for which the U.S. service provider *did not receive a fee,* prohibiting only the former. After all, both exportations have the same impact *in Iran.*"

Id. (emphasis in the original). The Court further observed that imposing a fee requirement would lead to anomalous results, "such as permitting a U.S. entity to render uncompensated legal or consulting services to an Iranian corporation." *Id.* In fact, a fee requirement "would provide a dangerous and unintended loophole for persons in the United States who are motivated to export services" to countries like Iran and North Korea "without regard to monetary compensation, "including those seeking to foster the very actions and policies that prompted the establishment" of the sanctions against countries like Iran and North Korea. *Id.* Under binding precedent, the fact that Griffith did not receive a fee is not a basis for dismissing the indictment.

Griffith's third argument is that he did not provide a service because his presentation had no economic value to the DPRK. (Mot. to Dismiss at 15 ("The common ground among all these definitions is the idea that a service is procured or commanded by a party, for that procuring party's economic benefit.")). Again, this is both incorrect and not a basis for dismissal. The purpose of the Conference was made clear to Griffith: to allow the DPRK and North Korean citizens to increase their understanding about blockchain and cryptocurrency technologies so that they could evade and avoid the crippling economic sanctions imposed by the United States. The DPRK would clearly derive value—economic and otherwise—if they were able to use blockchain and cryptocurrency technologies to evade U.S. sanctions. And as the text messages summarized above make clear, Griffith understood the value that he provided. For instance, Griffith knew that he was safe in North Korea, because "DPRK wouldn't want to scare away Blockchain talent that'll let them get around sanctions."

All of the defendant's arguments for why his conduct did not constitute a service to the DPRK are unavailing. A simple hypothetical lays bare the absurdity of Griffith's position. By Griffith's logic, the NKSR would permit an American physicist to travel to the DPRK and explain

the science behind nuclear weapons to a conference of North Korean physicists, so long as the science could be found on the Internet, he received no fee, and the regime's desire to build nuclear weapons was not economic in nature. Griffith's interpretation of "services" does not comport with the broader text and purpose of the NKSR.

Finally, even if Griffith's cramped interpretation of services were correct, the defendant's arguments would nonetheless fail because he is charged with a conspiracy, not a substantive violation of IEEPA. To convict Griffith on the sole count of the Indictment, the Government must only prove that the defendant willfully agreed to violate IEEPA with the intent that the conspiracy succeed. *See* Jury Instructions, *United States v. Zarrab*, 15 Cr. 867 (RMB), Dkt. 434 (Dec. 20, 2017 S.D.N.Y.). The defendant need not have actually succeeded in violating IEEPA. In a footnote, the defendant attempts to dismiss the lack of a substantive IEEPA charge as irrelevant to the analysis, since the Indictment must allege "that the intended future conduct the conspirators agreed upon includes all the elements of the substantive crime." (Mot. to Dismiss at 16 n.19 (quoting *United States v. Coplan*, 703 F.3d 46, 66 (2d Cir. 2012))). The Indictment alleges the elements of the substantive offenses that were the objects of the conspiracy—violating the sanctions and evading the sanctions. *See* Indictment ¶¶ 2-3. The jury could find that the Government proved that Griffith willfully agreed with others to violate or evade IEEPA and that he intended the conspiracy to succeed, but that the Government did not prove, for whatever reason, that the defendant's presentation actually constituted a substantive violation of IEEPA.[6]

[6] Griffith also cites to *United States v. Foote*, 413 F.3d 1240 (10th Cir. 2005), but that case is distinguishable. In *Foote*, the court found that the trademarks in which the defendant agreed to trade were not in use at the time of the crime and that, therefore, a conspiracy to violate the law could not have existed. *Id*. at 1249-50. The defendant here does not argue that he was *incapable* of violating sanctions when he agreed to attend and present at the conference, only that he did not in fact violate sanctions.

For the foregoing reasons, even if the Court looks beyond the face of the Indictment, the Government's proof at trial will establish that the defendant conspired to violate IEEPA by providing a service to the DPRK. Accordingly, the motion to dismiss should be denied.

D. Griffith's Presentation Does Not Fall Within the Informational Materials Exemption to the NKSR

Griffith next argues that his conduct falls within an exception to the NKSR for "information and informational materials not fully created and in existence at the date of the transactions." (Mot. to Dismiss at 17). This argument lacks merit, and the defendant's motion to dismiss on this ground should also be denied.

1. Applicable Law

In 1988, Congress amended IEEPA to exempt the regulation of "informational materials" from sanctions regulations. *See* Omnibus Trade and Competitiveness Act of 1988, Pub. L. No. 100–418, § 2502, 102 Stat. 1107, 1371 (1988) (codified at 50 U.S.C. app. § 5(b), 50 U.S.C. § 1702(b)) (the "Berman Amendment"). Accordingly, after the Berman Amendment, the "authority granted to the President by [IEEPA] does not include the authority to regulate or prohibit, directly or indirectly . . . the exportation to any country . . . of any information or informational materials, including but not limited to, publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds." 50 U.S.C. § 1702(b)(3).

In 1989, OFAC issued regulations interpreting the Berman Amendment. Consistent with the statute, the term "information or information materials" is defined to include "publications, films, posters, phonograph records, photographs, microfilms, microfiche, tapes, compact disks, CD ROMs, artworks, and news wire feeds." 31 C.F.R. § 510.312(a)(1). Moreover, since 1989, and thus at all times relevant to this case, the regulations have stated that the exemption for

information materials does not apply to "transactions related to information or informational materials *not fully created and in existence at the date of the transactions*, or to the substantive or artistic alteration or enhancement of information or informational materials, or to the provision of marketing and business consulting services." 31 C.F.R. § 510.213(c)(2) (emphasis added).

In 1994, Congress enacted the Free Trade in Ideas Act ("FTIA"), which amended IEEPA's informational materials exemption to override OFAC's ability to regulate "intangible items," by restricting the Executive from regulating transactions concerning such materials "regardless of format or medium of transmission." *See* Pub. L. No. 103–236, § 525, 108 Stat. 382, 474 (1994) (codified as amended at 12 U.S.C. § 95a, 50 U.S.C. § 1702(b)). Notably, however, the FTIA did not direct OFAC to change the relevant regulation here—namely, OFAC's exemption only of informational materials that are "fully created and in existence at the date of the transactions." 31 C.F.R. § 510.213(c)(2). This regulation has not changed since 1989.

2. Griffith's Presentation Was Not Fully Created and in Existence at the Time It Was Provided to the DPRK

Griffith's conduct is not exempted from the DPRK sanctions by the Berman Amendment, because Griffith's presentation and his answers to questions from the audience were not "fully created and in existence" at the time they were provided to the DPRK. Unlike a publication, film, or poster, Griffith created his presentation specifically for the DPRK's Conference, drew on a whiteboard to illustrate his points, and answered the questions posed to him in real-time.

The "Berman Amendment was considered 'a reaction to several seizures by the United States of shipments of magazines and books from embargoed countries and to the Treasury Department's restrictions on the permissible forms of payment for informational materials purchased from Cuba.'" *United States v. Amirnazmi*, 645 F.3d 564, 584 (3d Cir. 2011) (quoting *Kalantari v. NITV, Inc.*, 352 F.3d 1202, 1205 (9th Cir. 2003)). Accordingly, as the *Amirnazmi*

court explained in the context of a motion for a new trial based on violations of Iranian sanctions, "the key distinction rests between informational materials that are widely circulated in a standardized format and those that are *bespoke*." *Amirnazmi*, 645 F.3d at 587 (emphasis added). OFAC is not permitted to "regulate the sale or transfer of prefabricated or mass-produced informational materials," but it may prohibit the transfer of "custom-made materials crafted to suit the unique specifications of a particular purchaser." *Id.* "This distinction is sensible, and it reflects a permissible implementation of the statutory exemption in light of IEEPA's competing imperatives (i.e. restricting material support for hostile regimes while encouraging the robust interchange of information)." *Id.*

Because Griffith's presentation and his answers to questions were "bespoke" and created for the DPRK's specific interests and pre-approved topics, the services he provided to the DPRK do not fall within the informational materials exemption. As explained in detail above, Griffith did not simply read an academic paper to the audience at the Conference. Rather, Griffith's remarks on blockchain and cryptocurrency technologies, and his answers to questions during the Conference, educated the North Korean attendees on how they could use those technologies to avoid and evade U.S. sanctions against North Korea. These remarks clarified, for example, Griffith's explanation of blockchain technology, and provided advice on which other nations might be willing to serve North Korean individuals on over-the-counter exchanges. (*See* USAO_002645 ("And if China doesn't work, Singapore will probably be able to do it.")).

The recordings from the Conference and Griffith's own admissions establish that Griffith's remarks do not fit within the informational materials exemption. Griffith explained to the FBI that he created a presentation for the Conference, which used the content that the DPRK approved, and which addressed the topics that CC-2 told Griffith the Conference attendees would be most

interested in—namely, using these technologies to evade and avoid U.S. sanctions.[7] Griffith explained that technical difficulties prevented the use of a PowerPoint presentation that he had prepared, so Griffith used a whiteboard and drew diagrams instead. These diagrams, and Griffith's answers to questions, were plainly not "fully created and in existence" before the Conference.

Although the Court should not look beyond the allegations in the Indictment at the motion to dismiss stage, the Government submits that the evidence at trial will establish that Griffith's remarks at the Conference, whiteboard drawings, and answers to North Korean attendees questions were "crafted to suit the unique specifications" of the North Koreans in attendance at the Conference with approval from the DPRK's Government. *Amirnazmi*, 645 F.3d at 587. Moreover, Griffith does not claim—nor can he—that his presentation or his answers to questions were "prefabricated or mass-produced informational materials." *Id.* Accordingly, Griffith's presentation and answers to questions do not fall under the informational materials exemption to the NKSR.

3. OFAC's Interpretation of the "Informational Materials" Exemption is Permissible

In the alternative, Griffith asserts that OFAC's informational materials regulation, *see* 31 C.F.R. § 510.213(c)(2), is an impermissible agency interpretation of the Berman Amendment. (Mot. to Dismiss at 18-19). This argument is unsupported and does not provide a basis for dismissing the Indictment.

The defendant cites to no cases in this Circuit or District to support this argument, and the Government similarly has not found any on-point cases from this Circuit or District. The case the

[7] The defendant asserts that he has "regularly given presentations and spoken on panels at conferences throughout the world" (Mot. Dismiss at 3), but he has not provided any evidence that his presentation and answers to questions at the DPRK Conference were identical or even closely related to remarks he has given at other panels and conferences.

defense does cite—*Amirnazmi* from the Third Circuit—rejected the same argument in the context of the Iran sanctions regime. In *Amirnazmi*, the defendant provided Iran with a software tool that conveyed pricing and scientific information; he was convicted at trial for violating IEEPA. *Amirnazmi*, 645 F.3d at 570-71. On appeal, the defendant asserted that "OFAC's regulation removing informational materials 'not fully created and in existence at the date of the transactions' from the scope of the statutory exemption reflects an impermissible agency interpretation that should be struck down under the principles enunciated in *Chevron U.S.A. v. Natural Resources Defense Council, Inc.*, 467 U.S. 837, 842-42 (1984)." *Amirnazmi*, 645 F.3d at 583.

The regulation challenged by the defendant had been in effect since 1989, and neither Congress nor OFAC had chosen to repeal or change it. *Id*. at 587. The defendant asserts that the FTIA has "taken aim at OFAC's narrow interpretation of the Berman Amendment." (Mot. to Dismiss at 19). But the FTIA merely responded to "OFAC's exclusion of intangible materials from the definition of 'informational materials' by amending IEEPA's exemption" to apply to informational materials "regardless of format or medium of transmission." *Amirnazmi*, 645 F.3d at 585. Congress's focus on that aspect of OFAC's definition does not bear on the pertinent issue here, which is whether OFAC's interpretation that that the Berman Amendment does not exempt from regulation "informational materials not fully created and in existence at the date of the transactions," 31 C.F.R. § 510.213(c)(2), is entitled to *Chevron* deference. And with respect to that issue, as the *Amirnazmi* court held, "OFAC's interpretation of IEEPA's informational-materials exemption is 'based on a permissible construction of the statute.'" *Amirnazmi*, 645 F.3d at 586 (citation omitted). As the court observed, Congress's purpose in passing the Berman Amendment was to "ensure the robust exchange of informational materials would not be unduly inhibited by OFAC." *Id.* That purpose was served by allowing for the exchange of magazines and

books, and it was thus reasonable for OFAC to limit the exemption to those materials that were, like books and magazines, "fully created and in existence at the date of the transactions." 31 C.F.R. § 510.213(c)(2).

Moreover, as the *Amirnazmi* court observed, when the FTIA was passed, "Congress could have inserted text stipulating that the Executive may not regulate informational materials regardless of whether fully created and in existence at the date of the transactions." *Amirnazmi*, 645 F.3d at 587. In other words, Congress could have simply directed OFAC to change the pertinent regulation. "[C]ongressional failure to revise or repeal the agency's interpretation is persuasive evidence that the interpretation is the one intended by Congress." *Young v. Community Nutrition Institute*, 476 U.S. 974, 983, (1986) (quoting *NLRB v. Bell Aerospace Co.*, 416 U.S. 267, 275 (1974)); *see also United States v. Rutherford*, 442 U.S. 544, 554 n. 10 (1979) (noting that once an agency's statutory interpretation has been "fully brought to the attention of the public and the Congress, and the latter has not sought to alter that interpretation although it has amended the statute in other respects, then presumably the legislative intent has been correctly discerned" (internal citations and quotation marks omitted)); *Amirnazmi*, 645 F.3d at 587 ("When Congress is aware of an agency's interpretation of a statute and takes no action to correct it while amending other portions of the statute, it may be inferred that the agency's interpretation is consistent with congressional intent.") (internal quotation marks and alterations omitted)).

There is also "ample evidence to suggest Congress has accepted OFAC's decision to permit the circulation of informational materials already in existence while concomitantly regulating transactions that contemplate the creation of new materials." *Amirnazmi*, 645 F.3d at 587. As the *Amirnazmi* court concluded, the distinction between "prefabricated or mass-produced information materials" and "custom-made materials crafted to suit the unique specifications of a particular

purchaser" is "sensible," and "reflects a permissible implementation of the statutory exemption in light of IEEPA's competing imperatives (i.e. restricting material support for hostile regimes while encouraging the robust interchange of information)." *Id.* The court therefore concluded that OFAC's regulation setting forth the "not fully created and in existence at the date of the transactions" test is "a permissible construction of IEEPA's informational-materials exemption and is worthy of deference under [*Chevron*]." *Id.*

This Court should adopt the Third Circuit's persuasive reasoning and conclude that OFAC's regulation codified at 31 C.F.R. § 560.213(c)(2) is a permissible agency interpretation. Because the Indictment is facially sufficient, the regulation is permissible, and the evidence at trial will establish that Griffith's presentation and answers to questions were not "fully created and in existence at the date of the transactions," this Court should deny the defendant's motion to dismiss.

E. Griffith's Conduct is Not Protected by the First or Fifth Amendments

Finally, the defendant asserts that the First and Fifth Amendments to the U.S. Constitution bar this prosecution. (Mot. to Dismiss at 20-25). The defendant's motion to dismiss on these constitutional grounds should also be denied.

1. Griffith's First Amendment Challenge Should Be Rejected

Griffith claims that the Indictment should be dismissed because IEEPA, as applied to the facts here, "seeks to criminalize pure speech." (Mot. to Dismiss at 20). While Griffith surely has First Amendment rights as a U.S. citizen, it is well-established that speech can cross the line to criminal conduct. *See United States v. Rahman*, 189 F.3d 88, 117 (2d Cir. 1999) ("Numerous crimes under the federal criminal code are, or can be, committed by speech alone[,] . . . [b]ut if the evidence shows that the speeches crossed the line into criminal solicitation, procurement of criminal activity, or conspiracy to violate the laws, the prosecution is permissible.").

Griffith is charged with conspiring with others to provide services in the DPRK and evading and avoiding U.S. sanctions against the DPRK. Griffith's conduct does not constitute "pure speech." Yet, even assuming that strict scrutiny applies, IEEPA and the NKSR, as applied to the facts in this case, are narrowly tailored to serve a compelling government interest. Accordingly, the defendant's First Amendment claim should be rejected.

a. Applicable Law

To address a First Amendment as-applied challenge, a court must first determine the appropriate level of scrutiny to apply. *Reed v. Town of Gilbert*, 135 S. Ct. 2218, 2227 (2015). If a restriction is not content-based and only incidentally restricts expressive activity, it is subject to intermediate scrutiny. *See United States v. O'Brien*, 391 U.S. 367, 377 (1968). The regulation of expressive activity "is content-neutral so long as it is *justified* without reference to the content of the regulated speech." *Ward v. Rock Against Racism*, 491 U.S. 781, 791 (1989) (emphasis in original) (internal citations and quotation marks omitted). Whether a regulation is content neutral "centers on the purpose of the government regulation, that is, whether the government has adopted a regulation of speech because of disagreement with the message it conveys." *Emergency Coalition to Defend Educ. Travel v. U.S. Dep't of the Treasury*, 545 F.3d 4, 12 (D.C. Cir. 2008) (internal quotations and citations omitted). Under the test set forth in *O'Brien*, governmental action passes intermediate scrutiny if (1) "it is within the constitutional power of the Government"; (2) "it furthers an important governmental interest"; (3) "the governmental interest is unrelated to the suppression of expression"; and (4) "the incidental restriction on alleged First Amendment freedoms is no greater than is essential to the furtherance of that interest." 391 U.S. at 377.

However, where a law is "directed at conduct," but "the conduct triggering coverage under the statute consists of communicating a message" as applied to a defendant, strict scrutiny applies.

Holder v. Humanitarian Law Project, 561 U.S. 1, 28 (2010). A content-based restriction on protected speech "will be tolerated only upon a showing that it is narrowly tailored to a compelling government interest." *Time Warner Cable Inc. v. F.C.C.*, 729 F.3d 137, 155 (2d Cir. 2013) (citing *Turner Broad. Sys., Inc. v. F.C.C.*, 512 U.S. at 642, 653, 658 (1994)).

Holder v. Humanitarian Law Project involved a challenge to 18 U.S.C. § 2339B, which prohibits providing material support to a foreign terrorist organization ("FTO"). The plaintiffs there sought to provide material support to two designated FTOs by providing training on using law and political advocacy to resolve disputes and to negotiate peace agreements. Under Section 2339B, however, "material support" includes imparting a specific skill, or communicating advice "derived from specialized knowledge," whereas speech "[was] not barred if it impart[ed] only general or unspecialized knowledge." *Humanitarian Law Project*, 561 U.S. at 27. The Supreme Court observed that while the material support statute could be "described as directed at conduct[,] . . . as applied to plaintiffs the conduct triggering coverage under the statute consists of communicating a message." *Id.* at 28. Accordingly, because the Supreme Court found that the material support statute regulated speech on the basis of its content, it applied strict scrutiny.

The Court in *Humanitarian Law Project* nonetheless concluded that the prohibition at issue survived strict scrutiny. 561 U.S. at 31. The Court held that the Government had a compelling interest in combatting international terrorism, and that prohibiting the proposed support to an FTO was narrowly tailored, since it "is wholly foreseeable that the [FTO] could use the specific skills that plaintiffs propose to impart as part of a broader strategy to promote terrorism" by, "for example, pursu[ing] peaceful negotiation as a means of buying time to recover from short-term setbacks, lulling opponents into complacency, and ultimately preparing for renewed attacks." *Id.* at 36-37 (internal citations and quotation marks omitted). The Court described these possibilities

as "real, not remote." *Id*. at 37. The Court therefore concluded that Section 2339B—even as applied to the speech at issue in *Humanitarian Law Project*—did not violate the First Amendment. *Id*.

At least one court has rejected a First Amendment challenge to IEEPA following the Supreme Court's *Humanitarian Law Project* decision. In *Kadi v. Geithner*, 42 F. Supp. 3d 1 (D.D.C. 2012), the petitioner challenged his designation as a Specially Designated Global Terrorist ("SDGT"), and the related blocking of his financial transactions under IEEPA, claiming, among other things, that IEEPA violated the First Amendment as applied to him. The *Kadi* court applied intermediate scrutiny and rejected the petitioner's First Amendment claim. *Id.* at 34. The court also explained that it would have reached the same result under strict scrutiny, because "the sensitive interests of national security and foreign affairs at stake" in combatting terrorism constituted a compelling government interest, and "because all contributions to foreign terrorist organizations (regardless of any benign intent) could further terrorism." *Id.* at 35. "[E]ven allowing for good-intentioned financial support to organizations and individuals involved in terrorism would be problematic, as organizations could free up other resources to be used towards violent terrorist objectives." *Id.*; *see also Holy Land Found. for Relief & Dev. v. Ashcroft*, 333 F.3d 156, 165 (D.C. Cir. 2003) ("[T]he law is established that there is no constitutional right to fund terrorism."); *Islamic Am. Relief Agency v. Gonzales*, 477 F.3d 728, 735 (D.C. Cir. 2007) (stating that "there is no constitutional right to fund terrorism," and that "where an organization is found to have supported terrorism, government actions to suspend that support are not unconstitutional"); *cf. United States v. Dhafir*, 5:03-CR-64, 2003 WL 27383007 at *5 (N.D.N.Y. July 3, 2003) (rejecting a First Amendment free exercise challenge to IEEPA, as the defendant's

"interest in the free exercise of his religious duties is outweighed by the legitimate and compelling security interests of the United States").

b. Discussion

As described above, as-applied challenges to content-neutral regulations are ordinarily subject to intermediate scrutiny. *See Ward*, 491 U.S. at 791. In *Kadi*, the court agreed with the Government that intermediate scrutiny was the appropriate test to a First Amendment challenge to IEEPA, because the petitioner there made no claim that he sought to donate to the entities and individuals involved in that case "for political reasons," or that he sought "to engage in any other activities of the type that were at issue in [*Humanitarian Law Project*] or [*Al Haramain*]." 42 F. Supp. 3d at 34. Applying intermediate scrutiny, the court concluded that the Government had the authority to designate Kadi as a SDGT and to freeze or block assets that fall under U.S. jurisdiction, because "blocking or freezing assets that may be used to support terrorists and/or terrorist activities furthers an important government interest—'combating terrorism by undermining its financial base.'" *Id.* (quoting *Holy Land Found.*, 333 F.3d at 161).

As the Court observed, "the designation of Kadi as a SDGT and the blocking of his assets merely restricts his ability to make financial transfers to other SDGTs, not his ability to express his views generally." *Id.* Similarly, in this case, the restriction on Griffith's ability to conspire with others to provide services to the DPRK or to evade and avoid sanctions against the DPRK did not impact Griffith's ability to express his views on blockchain and cryptocurrency technologies more generally. The incidental restriction on First Amendment freedoms in this case "is no greater than is essential to the furtherance of the strong governmental interest." *Id.*

The defendant asserts that as applied here, the Indictment "seeks to criminalize pure speech." (Mot. to Dismiss at 20). This argument ignores all of the other acts the defendant took

during his conspiracy to provide services to the DPRK, and to evade and avoid the U.S. sanctions. As summarized above, the defendant's conduct included, among other things: securing a visa to the DPRK, traveling to the DPRK, attending the Conference, attempting to coordinate the exchange of cryptocurrency between South and North Korea, attempting to provide the DPRK with a "node" that could be used to validate and relay cryptocurrency transactions, exploring the purchase of North Korean domain names, recruiting others to attend future DPRK conferences, and pitching his company to the Conference attendees. (*See* USAO_002621 (stating that one of the most valuable things that Ethereum can offer the DPRK is providing payments "that the USA can't stop")). The defendant's criminal conduct went well beyond his remarks at the Conference.

In any event, however, the Court need not resolve whether intermediate or strict scrutiny should apply, because the defendant's First Amendment claim fails either way. As applied to the conduct in this case, IEEPA and the NKSR also satisfy strict scrutiny.

It is well established that maintenance of national security is a "public interest of the highest order." *Am. Civil Liberties Union v. Clapper*, 785 F.3d 787, 826 (2d Cir. 2015); *see also Haig v. Agee*, 453 U.S. 280, 292 (1981) (explaining that matters relating to the conduct of foreign relations "are so exclusively entrusted to the political branches of government as to be largely immune from judicial inquiry or interference") (internal citations and quotation marks omitted); *Stagg P.C. v. United States Dep't of State*, 673 F. App'x 93, 95-96 (2d Cir. 2016) ("[M]atters of national security . . . present the most compelling national interest . . . ."). In authorizing the NKSR, the President noted that the situation on "the Korean Peninsula constitute[s] an unusual and extraordinary threat to the national security and foreign policy of the United States." (Exec. Order 13466). Later Executive Orders cited the need to combat North Korean nuclear proliferation, money laundering, counterfeiting, bulk cash smuggling, narcotics trafficking, coercive cyber

actions, and serious human rights abuses, all of which "constitute a continuing threat to the national security, foreign policy, and economy of the United States. (Exec. Orders 13466, 13551, 13687, 13722). Congress has also identified the DPRK as posing a significant national security threat to the United States. *See* 22 U.S.C. § 9201(a)(9) (stating that the conduct of "the Government of North Korea poses an imminent threat to . . . (A) the security of the United States and its allies; (B) the global economy; (C) the safety of members of the United States Armed Forces; (D) the integrity of the global financial system; (E) the integrity of global nonproliferation programs; and (F) the people of North Korea."); 22 U.S.C. § 9201(a)(3) (stating that the "Government of North Korea has been implicated repeatedly in money laundering and other illicit activities, including—(A) prohibited arms sales; (B) narcotics trafficking; (C) the counterfeiting of United States currency; (D) significant activities undermining cybersecurity; and (E) the counterfeiting of intellectual property of United States persons").

There is plainly a compelling state interest in addressing these threats to national security. And Griffith's own text messages establish that the defendant knew that the services he was providing to the DPRK could be used to evade sanctions and exacerbate these risks to national security, including drug trafficking and the proliferation of nuclear weapons. (*See supra* (stating that an Ethereum node would make economic sense, because it'll "help [the DPRK] circumvent the current sanctions on them"); (the "DPRK wouldn't want to scare away Blockchain talent that'll let them get around sanctions"); (in response to the question, "[w]hat if [the DPRK is] funding their drug trade and nuclear program with crypto," Griffith responded "Unlikely. But they'd probably like to start doing such.")). Griffith plainly knew that the services he was providing could be used to finance the DPRK's nuclear program and to facilitate criminal conduct.

As applied to the conduct here, the Government therefore has a compelling interest in ensuring that cryptocurrency technologies and methods are not provided, transferred, facilitated, taught or even explained to the DPRK and North Korean citizens, because those technologies could then be used to evade sanctions and to help the DPRK raise money for illicit purposes. As in *Kadi*, "because all contributions to foreign terrorist organizations (regardless of any benign intent) could further terrorism, the Government has a compelling interest in ensuring that such support not reach these organizations." 42 F. Supp. 3d at 35. Even assuming that Griffith's services were "benign"—which is rebutted by his own text messages and the content of his presentation—they could still facilitate and further the national security threats posed by the DPRK. The Government has a compelling interest in restricting U.S. persons from providing such services to the DPRK.

Moreover, the sanctions regime is itself narrowly tailored to address this threat. While the NKSR prohibits U.S. persons from providing services to the DPRK, it allows for the provision of "informational materials" that are fully created and in existence at the time of the transfer. This First Amendment safe harbor underscores the desire by Congress and OFAC to ensure that the NKSR regulations are not needlessly restrictive of speech. Moreover, as the court in *Kadi* observed, the OFAC regime at issue there "provides for the listing of a limited number of SDGTs, permits entities and individuals to contest their designations, and allows the Government to delist individuals and entities and remove their SDGT designations." *Kadi*, 42 F. Supp. 3d at 35. In that way, the sanction regime has a "natural stopping place" for the reach of the statute. *Humanitarian Law Project*, 561 U.S. at 31. Here, OFAC also permits individuals to obtain licenses to perform acts that would otherwise violate sanctions, and only criminalizes the provision of services when the defendant "willfully" violates the law. These features of IEEPA and the NKSR regulations

underscore that the prohibition on providing services to the DPRK is targeted towards combatting conduct that poses a national security threat, without unduly limiting innocent speech.

Griffith's conduct also "helped lend legitimacy" to the DPRK, and made it easier for the DPRK to "raise funds" by accessing the international financial system, notwithstanding U.S. sanctions. *Humanitarian Law Project*, 561 U.S. at 30. Like money, services are "fungible," and Griffith did not have control over the purposes to which the DPRK would put the services that Griffith provided. *Id.* at 31. It was thus "wholly foreseeable" that providing information to the DPRK and North Koreans about blockchain and cryptocurrency technologies would provide information that could be used to evade and avoid U.S. sanctions. *Id*. Congress can, consistent with the First Amendment, prohibit this direct provision of services. *See id.* at 36-37 ("It is wholly foreseeable that the PKK could use the specific skills that plaintiffs propose to impart . . . as part of a broader strategy to promote terrorism.") (internal quotation marks and alterations omitted).

The Ninth Circuit's decision in *Al Haramain Islamic Found., Inc. v. U.S. Dep't of Treasury*, 686 F.3d 965 (9th Cir. 2012) does not alter the analysis. That case addressed whether criminalizing advocacy on behalf of a designated terrorist organization violated the First Amendment. In particular, the plaintiff sought to "speak[ ] to the press, hold[ ] demonstrations, and contact[ ] the government" on behalf of the terrorist organization, activities that implicated the apex of First Amendment protections. *Id.* at 1001. The Ninth Circuit, in ruling for the petitioner, distinguished *Humanitarian Law Project* on several grounds, none of which apply here. First, the Ninth Circuit held that "the connection between the provision of services and the freeing of funds for terrorist activities is much more attenuated here than in [*Humanitarian Law Project*]." *Id.* at 999. Here, by contrast, the threat that the DPRK could use knowledge of blockchain and cryptocurrency technologies to obtain funding outside of the international banking system is not at all attenuated

from the service Griffith provided. Second, the Ninth Circuit minimized the concern that coordinated advocacy would help "legitimize a terrorist organization." *Id.* at 1000 (noting that on the facts in that case, "this rationale is not particularly strong."). By contrast, here, facilitating the DPRK's access to the international financial system and providing a currency that it could use to participate in vital legitimate-seeming commercial activities (even non-criminal ones) was a much more legitimacy-enhancing service than those at issue in *Al Haramain* or even *Humanitarian Law Project*. Finally, the Ninth Circuit relied on the fact that OFAC relied only on "*past* conduct by *other* branches" of the larger organization, as opposed to "ongoing conflicts between the foreign organization and an ally of the United States. *Id.* By contrast, here there can be no serious dispute that the DPRK poses a continuing threat, and that letting U.S. persons like Griffith provide services to the DPRK would undermine foreign affairs efforts involving other countries and multi-national organizations like the United Nations, which are working to combat that threat.

In short, the factors at issue in *Al Haramain* are not present here. Griffith provided technical services directly to the DPRK, a hostile foreign power, not a domestic branch of an international organization. *See Capital Cities/ABC, Inc. v. Brady*, 740 F. Supp. 1007, 1012 (S.D.N.Y. 1990) (rejecting the premise that "the congressional or executive power to regulate speech when dealing with foreign affairs is subject to the same scrutiny and limitations that the First Amendment would impose in the domestic context."); *see also Teague v. Regional Commissioner of Customs*, 404 F.2d 441, 445-46 (2d Cir. 1968) (upholding, under intermediate scrutiny, the Cuban embargo).

Accordingly, as applied here, the NKSR survives strict scrutiny. Griffith attended the Conference for the express purpose of explaining blockchain and cryptocurrency technologies to a group of 100 North Koreans of varying technical ability and knowledge. He knew in advance

that this audience would be most interested in how those technologies could be used to evade and avoid sanctions, and to commit money laundering, and he tailored his remarks accordingly. Griffith specifically explained how these technologies could be used to transfer money outside of the international banking system and around U.S. sanctions. As in *Humanitarian Law Project*, it "is wholly foreseeable that [the DPRK and its citizens] could use the specific skills" that Griffith imparted "as part of a broader strategy" to evade and avoid U.S. sanctions. 561 U.S. at 37. The risk that the DPRK could and would use this technical information to evade sanctions was "real, not remote." *Id.* at 37. Because the NKSR is narrowly tailored to serve a compelling state interest, applying the regulations to prohibit Griffith's conduct does not violate the First Amendment. Accordingly, the defendant's motion to dismiss on First Amendment grounds should be denied.

2. Griffiths' Fifth Amendment Challenge Should Be Rejected

Finally, the defendant asserts that the Indictment should be dismissed because Griffith "did not have fair warning that OFAC or the Department of Justice would contend that his alleged pure-speech conduct constituted a crime." (Mot. to Dismiss at 24). This argument is wrong as a matter of law and refuted by the facts of this case.

a. Applicable Law

"To satisfy the Fifth Amendment's due process requirements, a penal statute must 'define the criminal offense [1] with sufficient definiteness that ordinary people can understand what conduct is prohibited and [2] in a manner that does not encourage arbitrary and discriminatory enforcement.'" *United States v. Roberts*, 363 F.3d 118, 122 (2d Cir. 2004) (quoting *Kolender v. Lawson*, 461 U.S. 352, 357 (1983)). But where a statute "contains a scienter requirement," as IEEPA does, a defendant's "vagueness challenge must be met with some measure of skepticism, at least with regard to the 'fair notice' prong of *Kolender*." *Id.* at 123 (citing *Village of Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 499 (1982)); *see also id.* ("[A] scienter

requirement [in a criminal statute] may mitigate a law's vagueness, especially with respect to the adequacy of notice to the complainant that his conduct is proscribed."). In IEEPA prosecutions, "ignorance of the law is a defense; the inability to appreciate the meaning of the law negatives the mens rea required for conviction," and the defendant remains "free to . . . argue this to the jury." *Amirnazmi*, 645 F.3d at 589-90 (internal citation and quotation marks omitted).

When a statute "interferes with the right of free speech or of association, a more stringent vagueness test should apply," but "perfect clarity and precise guidance have never been required even of regulations that restrict expressive activity." *Humanitarian Law Project*, 561 U.S. at 18–19 (internal citations and quotations omitted). The Court in *Humanitarian Law Project* therefore rejected a due process challenge to the material support for terrorism statute, in addition to the related First Amendment challenge discussed above, finding that "a person of ordinary intelligence would understand the term 'service' to cover advocacy performed in coordination with, or at the direction of, a foreign terrorist organization." *Id*. at 24.

b. Discussion

The defendant focuses his due process challenge on the meaning of the term "service," but IEEPA's mens rea requirement is not, as a matter of law, "a slender reed." (Mot. to Dismiss at 25). Criminal penalties under IEEPA are reserved for those who "willfully commit[], willfully attempt[] to commit, or willfully conspire[ ] to commit" a violation of any license, order or regulation issued pursuant to IEEPA. 50 U.S.C. § 1705(c). IEEPA expressly exempts those who act in "good faith" reliance on IEEPA, or on "any regulation, instruction, or direction" issued under IEEPA, from both civil and criminal liability. *Id.* § 1702(a)(3). Courts have therefore repeatedly rejected due process challenges to IEEPA prosecutions, because this heightened scienter requirement of willfulness alleviates the risk of convicting a defendant who unwittingly violates

the law. *See, e.g.*, *Amirnazmi*, 645 F.3d at 589-90; *United States v. Zhi Yong Guo*, 634 F.3d 1119, 1123 (9th Cir. 2011); *see also United States v. All Funds on Deposit in United Bank of Switzerland*, No. 01 CIV. 2091 (JSR), 2003 WL 56999, at *1 (S.D.N.Y. Jan. 7, 2003) (rejecting due process challenge to IEEPA violation relating to the provision of "services," though referencing a pre-*Banki* definition of the term); *United States v. Quinn*, 401 F.Supp.2d 80, 100-01 (D.D.C. 2005) (rejecting a vagueness challenge to the export administration regulations because "concerns about defendants being convicted under a law that they could not have reasonably understood are alleviated" by the scienter requirement).

At trial, Griffith's own statements and actions will establish that Griffith acted willfully. As explained in detail above, Griffith exchanged text messages with others that showed his intent to help the DPRK and its citizens evade and avoid U.S. sanctions, and his understanding that evading sanctions would be valuable to the DPRK. Griffith also told law enforcement agents that he knew that the Conference presentations were supposed to address the potential use of blockchain and cryptocurrency technologies to evade U.S. sanctions, and that he crafted a presentation that was consistent with this directive. The recordings from the Conference also show that Griffith explained to an audience of approximately 100 North Koreans how they could use these technologies to transfer money outside of the international banking system, which Griffith knew violated U.S. sanctions. In short, the evidence will establish that Griffith willfully conspired with others to provide the DPRK with services, and to evade and avoid U.S. sanctions.

While the NKSR does not expressly define the term service, the "plain and unambiguous meaning" of that term plainly covers Griffith's actions in this case, particularly when taking account of the "broader text and purpose" of the sanctions regime. *Banki*, 685 F.3d at 107 (internal citation and quotation marks omitted). In particular, service "refers to concerted activity, not

independent advocacy." *Humanitarian Law Project*, 561 U.S. at 23. Here, Griffith provided a service *to* the DPRK—the "word 'to' indicates a connection between the service and the foreign group." *Id.* at 24. There could be no lack of notice, because "a person of ordinary intelligence would understand that independently advocating for a cause is different from providing a service to a group that is advocating for that cause." *Id.* Moreover, while "independent advocacy" is not prohibited, "a person of ordinary intelligence would understand the term 'service' to cover advocacy performed in coordination with, or at the direction of," a sanctioned country like the DPRK. *Id.* In short, as in *Humanitarian Law Project*, the statute and regulations are sufficiently clear in their application to the defendant's conduct, and so the defendant's "vagueness challenge must fail." *Id.* at 21.

As a matter of Fifth Amendment Due Process, there is no lack of fair notice when the evidence shows the "defendants actually believed what they were doing was illegal." *Roberts*, 363 F.3d at 123 (internal citation omitted). The evidence will show that Griffith joined a conspiracy to help the DPRK evade sanctions, and that he repeatedly demonstrated that he knew he was violating the law. He admitted to law enforcement that he knew that the DPRK was under strict U.S. sanctions, and that travel to the DPRK was prohibited. The State Department denied his request to travel to the DPRK, but he went anyway. He took steps to create a cryptocurrency "node" in the DPRK, and explained in a text message that doing so made "economic sense" for the DPRK, because "[i]t'll help them circumvent the current sanctions on them." As the Supreme Court has held, a person "who engages in some conduct that is clearly proscribed cannot complain of the vagueness of the law as applied to the conduct of others." *Humanitarian Law Project*, 561 U.S. at 18-19 (internal quotation marks omitted) (quoting *Hoffman Estates v. Flipside, Hoffman Estates, Inc.*, 455 U.S. 489, 495 (1982)). In other words, a defendant "whose speech is clearly

proscribed cannot raise a successful vagueness claim under the Due Process Clause of the Fifth Amendment for lack of notice." *Id.* at 20.

On these facts, Griffith cannot seriously claim that dismissal is warranted, because he was surprised to learn that it is against U.S. law to conspire to provide services to a sanctioned country, and to evade and avoid U.S. sanctions. The evidence will establish that Griffith's conduct was both brazen and criminal. The motion to dismiss on Due Process grounds should be denied.[8]

II. THE MOTION FOR A BILL OF PARTICULARS SHOULD BE DENIED

The defendant's request for a bill of particulars appears to seek: (1) the locations where acts or events in furtherance of the alleged conspiracy were committed; (2) the services the defendant and others provided to the DPRK and names of others who helped the defendant provide those services; and (3) the laws and regulations the defendant and his co-conspirators conspired to violate. This information is either not necessary to trial preparation or has been provided in the Complaint, Indictment, briefing in opposition to the defendant's motions, and in the extensive discovery produced so far in this case. In addition, the Government proposes to provide additional Section 3500 material 30 days prior to trial. Accordingly, the request for a bill of particulars should be denied.

A. Applicable Law

While Rule 7(f) of the Federal Rules of Criminal Procedure permits the Court to direct the Government to file a bill of particulars, the test is "whether the information sought is necessary,

[8] The defense also asserts that this prosecution violates due process because "OFAC officials did not initially support the prosecution." (Mot. to Dismiss at 24). As explained in greater detail below, however, *see infra*, the communications between the prosecution team and OFAC, which have been produced to the defense in discovery, show that OFAC determined that Griffith's conduct violated IEEPA and did not fall within the informational materials exemption provided by the Berman Amendment.

not whether it is helpful." *United States v. Facciolo*, 753 F. Supp. 449, 451 (S.D.N.Y. 1990), *aff'd sub nom. United States v. Skowronski*, 968 F.2d 242 (2d Cir. 1992) (superseded on other grounds); *see also United States v. Payden*, 613 F. Supp. 800, 816 (S.D.N.Y. 1985) ("[I]f the defendant has been given adequate notice of the charges against him, the government is not required to disclose additional details about its case."). Because "a bill of particulars confines the government's evidence at trial to the particulars furnished," they are generally disfavored. *Payden*, 613 F. Supp. at 816.

In the context of conspiracy allegations, "the defendant does not 'need' detailed evidence about the conspiracy in order to prepare for trial properly." *Feola*, 651 F. Supp. at 1132. Specifically, "defendants need not know the means by which it is claimed they performed acts in furtherance of the conspiracy nor the evidence which the Government intends to adduce to prove their criminal acts." *Id*. Thus, as the Second Circuit has stated, "[t]he Government need not, when charging conspiracy, set out with precision each and every act committed by the conspirators in the furtherance of the conspiracy." *Cohen*, 518 F.2d at 733; *see also Trippe*, 171 F. Supp. 2d at 240 ("[D]emands for particular information with respect to where, when, and with whom the Government will charge the defendant with conspiring are routinely denied."); *United States v. Matos-Peralta*, 691 F. Supp. 780, 791 (S.D.N.Y. 1988) ("With respect to conspiracy charges in particular, since the government is not required to prove exactly when or how a conspiracy was formed or when or how a particular defendant joined the scheme, and as the circumstantial proof on which the government usually relies to prove the existence of a scheme often does not reveal such details, the courts have consistently rejected demands for particulars as to the formation of a conspiracy or the entry into the conspiracy of a particular defendant or confederate.").

Courts faced with requests for such disclosures consider, among other factors, the number of co-conspirators, the duration and breadth of the charged conspiracy, whether revealing the identity of co-conspirators would pose a risk to co-conspirator witnesses, whether other materials provide adequate notice of the charges, and the voluminousness of pretrial disclosures. *See United States v. Nachamie*, 91 F. Supp. 2d 565, 572 (S.D.N.Y. 2000) (setting forth factors); *United States v. Fruchter*, 104 F. Supp. 2d 289, 313 (S.D.N.Y. 2000) (explaining that a "request for names of all aiders, abettors, unindicted co-conspirators, and confidential informants is nothing more than a request for a witness list").

Furthermore, a bill of particulars is not required when the information the defendant seeks is provided in discovery. *See United States v. Binday*, 908 F. Supp. 2d 485, 497 (S.D.N.Y. 2012) ("If the information the defendant seeks 'is provided in the indictment or in some acceptable alternate form,' such as discovery or other correspondence, no bill of particulars is required." (quoting *United States v. Bortnovsky*, 820 F.2d 572 (2d Cir. 1987))).

A bill of particulars is not a "device for obtaining evidentiary detail." *United States v. Purcell*, No. 18CR81(DLC), 2018 WL 4378453, at *7-8 (S.D.N.Y. Sept. 13, 2018), *aff'd*, 967 F.3d 159 (2d Cir. 2020) . Rather, in deciding a motion for a bill of particulars, "[t]he important question is whether the information sought is necessary, not whether it is helpful." *Gonzalez*, 2004 WL 2297341, at *1-2 (internal quotation marks omitted) (quoting *United States v. Facciolo*, 753 F. Supp. 449, 451 (S.D.N.Y. 1990)). The Court should also consider both the charging instruments and the discovery provided to the defendant. *See Purcell*, 2018 WL 4378453, at *7-8 (citing *United States v. Torres*, 901 F.2d 205, 234 (2d Cir. 1990)). "Courts have been highly reluctant to require a bill of particulars when a defendant has asked for specific identities of co-conspirators or others allegedly involved." *Gonzalez*, 2004 WL 2297341, at *1-2.

B. Discussion

Between the facts contained in the Complaint and Indictment, and the discovery and disclosures provided to the defendant, the defendant has more than enough information available to him to prepare his defense and to avoid surprise at trial. *See Gonzalez*, 2004 WL 2297341, at *1-2 (citing *Torres*, 901 F.2d at 233-34 (upholding district court's denial of a bill of particulars where "a wealth of evidentiary detail from the discovery to date, including electronic intercepts, search evidence and exhaustive supporting affidavits")); *see also United States v. Rodriguez*, 1999 WL 820558 at *2 (S.D.N.Y. 1999) (denying motion for a bill of particulars identifying known co-conspirators where the indictment coupled with discovery allowed a defendant "both to prepare his defense and to avoid prejudicial surprise at trial").

The defendant claims that he needs a bill of particulars to identify his co-conspirators, events giving rise to venue in the Southern District of New York, and a "specific recitation" of the alleged services that the defendant conspired to provide in violation of U.S. sanctions on North Korea. However, the Government has provided the defense with sufficient information regarding these issues. The detailed Complaint and extensive discovery—including contemporaneous recordings of the defendant's remarks at the Conference, searchable extractions from numerous electronic devices, and early production of Section 3500 material, among other things—supply the defendant with ample information to understand the charges against him, to prepare a defense, and to protect against double jeopardy. Indeed, the defendant has already used his thorough access to this information to prepare a defense, such as by challenging the Government's evidence as to venue and the provision of services. (*See* Dkt. Nos. 43, 65).

As the defendant concedes, the Government has already confirmed the identities of two of the defendant's alleged co-conspirators (described here and in the Complaint as CC-1 and CC-2), and the identities of the other potential members of the conspiracy known to the Government—

such as the other identified conference participants and Griffith's North Korean government handler—are clearly disclosed in the discovery. The defendant was the only American citizen in this group, and thus the only "U.S. person" to whom the NKSR applied; the objects of the conspiracy therefore revolved primarily around his own conduct and those who agreed to facilitate his crime. While the Government is under no obligation to enumerate all members of the charged conspiracy at this stage, the Government has supplied the defendant with ample notice regarding the charged conduct in this case.

In stark contrast to the cases cited by the defendant in support of particulars identifying co-conspirators—the 23-defendant, 26-count RICO conspiracy charges spanning multiple complex fraud and bribery schemes by the Bonanno Crime Family of La Cosa Nostra, in *United States v. Lino*, No. 00 Cr. 632 (WHP), 2001 WL 8356 at *1, 12-13 (Jan. 2, 2001); the 19-defendant, 17-count charges in *United States v. Feola*, 651 F. Supp. 1068 (S.D.N.Y 1987); and a series of complex securities fraud conspiracies—this case involves a single defendant charged with one count of conspiring to violate U.S sanctions. Here, there are fewer known conspirators, the defendant served as the hub of the conspiracy because he was the sole U.S. person in the conspiracy subject to the NKSR, the duration of the conspiracy set forth in the Indictment was only about a year and a half, and it was centered on a weeklong event, the Conference, all of which is thoroughly disclosed and documented in the Complaint and the extensive discovery already provided. Under the *Nachamie* factors, the number of co-conspirators and the duration and breadth of the charged conspiracy plainly militate against a bill of particulars identifying co-conspirators because there is little risk of unfair surprise. *See Nachamie*, 91 F. Supp. 2d at 572. The defendant's motion for a bill of particulars identifying co-conspirators is meritless and should be denied.

Moreover, the defendant's claim that he needs a bill of particulars in order to facilitate his own witness interviews reveals that his motion is "nothing more than a request for a witness list." *Fruchter*, 104 F. Supp. 2d at 313; (Mot. for Particulars at 11, 12). But "it is well-settled that the Government is 'under no obligation to give [a defendant] advance warning of the witnesses who would testify against him.'" *United States v. Delacruz*, No. 14 CR 815 KBF, 2015 WL 2211943, at *3 (S.D.N.Y. May 12, 2015) (quoting *United States v. Alessi*, 638 F.2d 466, 481 (2d Cir. 1980)); *see also United States v. Freeman*, No. 18-CR-217 (KMW), 2019 WL 2590747, at *3 (S.D.N.Y. June 25, 2019) ("A defendant is not entitled to the Government's witness list prior to trial."); *United States v. Castellaneta*, No. 06 CR. 684 (GEL), 2006 WL 3392761, at *2 (S.D.N.Y. Nov. 20, 2006), at *2. The defendant cites no authority for the proposition that a bill of particulars should be ordered to assist the defendant in procuring witness interviews of individuals already known to him. The defendant knows the individuals he attended the Conference with, and he is in a position to pursue his own defense investigation if he wishes.

The Government has also outlined events occurring in the Southern District of New York in response to the defendant's motion to dismiss for lack of venue, and the Court denied the defendant's motion for a bill of particulars "addressed to venue" in connection with that motion. (*See* Dkt. 53 at 5). The defendant presents no new arguments justifying a bill of particulars as to venue now. As before, the defendant is aware of the Government's allegations, and the Government has produced discovery on this point—including, now, seized contents of an email account used by the defendant's co-conspirators at the DPRK Mission. Unlike in *United States v. Szur*, No. S5 97 Cr. 108 (JGK), 1998 WL 132942 (S.D.N.Y. Mar. 20, 1998), which involved a dispute over allegedly fraudulent documents in New Jersey, it is not "unclear" "what acts were committed in the Southern District of New York." *Id*. at *9. The defendant has all the information

to which he is entitled on this point. (Dkt. 46 at 3-6 (detailing evidence as to venue)). The defendant's request therefore rests on a single, improper objective—prematurely constraining the Government's proof at trial. *See, e.g.*, *Szur*, 1998 WL 132942 at *11 (citing *Muyet*, 945 F. Supp. at 599 ("It is improper to use a bill of particulars to compel the Government to disclose the manner in which it will prove the charges or preview its evidence or legal theory." (internal citation omitted)).

Lastly, the Complaint specifies in detail the services the defendant conspired to provide in violation of U.S. sanctions, such as Griffith's presentation at the DPRK Cryptocurrency Conference on "topics that were pre-approved by DPRK officials, provid[ing] the DPRK with valuable information on blockchain and cryptocurrency technologies, and participat[ing] in discussions regarding using cryptocurrency technologies to evade sanctions and launder money," in addition to later attempting to recruit other individuals to travel to the DPRK and "formulating plans to facilitate the exchange of Cryptocurrency-1 between the DPRK and South Korea." (Compl. ¶¶ 5, 15(f)-(j), 16(a)-(c), 17(a)-(c)). As explained in detail above, audio and video recordings of the defendant's remarks at the Conference, and the defendant's own admissions about this conduct, among other things, have already been produced in discovery. The dates, participants, and payments relating to this conduct are similarly transparent from the discovery, particularly, the defendant's own emails and text messages. The Government has produced witness statements, such as the statements of Witness-2, to provide the defendant with further clarity regarding the charged conduct, the Government's theory of the case, and the anticipated trial evidence. The Government has also thoroughly catalogued and labeled the discovery in letters to the defense, and has provided the discovery in a searchable format wherever possible. In this context, the defendant's bald claim that he has been sent on a "fishing expedition" to understand

the charges against him rings hollow. (Mot. for Particulars at 11). In light of the Complaint, the recordings, the search warrant affidavits, the defendant's admissions and communications, the witness statements, and extensive briefing (including this opposition), the defendant is on notice of the charges against him.

As courts in this Circuit have uniformly recognized, the detailed disclosures already provided to the defendant strongly militate against ordering a bill of particulars. *See, e.g.*, *United States* v. *Machado*, 986 F. Supp. 2d 288, 293 (S.D.N.Y. 2013) (denying bill of particulars where "[d]iscovery includes nearly four thousand audio recordings of intercepted calls with searchable line sheets of the calls identifying participant, date, and time of the calls, recordings of undercover purchases of narcotics, tracking and search warrant applications, and laboratory reports"); *United States v. Reinhold*, 994 F. Supp. 194, 201 (S.D.N.Y. 1998) (denying bill of particulars where the "indictment is detailed in its allegations" and the "defendants have had extensive discovery"); *United States v. Conesa*, 899 F. Supp. 172, 176 (S.D.N.Y. 1995) (denying bill of particulars where "[t]he Indictment sufficiently advises defendants of the specific acts of which they are accused" and "the Government . . . has made available to defense counsel extensive discovery that supplements the information provided in the . . . Indictment").

In sum, the defendant's motion for a bill of particulars appears to be little more than a request for further "evidentiary detail." *See Purcell*, 2018 WL 4378453, at *7-8. The defendant has more than sufficient information to understand the charges against him, to prepare a defense, and to protect against double jeopardy. Accordingly, the defendant's motion for a bill of particulars should be denied.[9]

[9] In advance of trial, the Government will also produce its witness list, its exhibit list, and any outstanding Section 3500 material, in accordance with the schedule set by the Court. This information will provide the defendant with timely access to even more information—such as the

III. THE MOTION TO COMPEL DISCOVERY SHOULD BE DENIED

The defendant's motion to compel seeks three categories of discovery: (1) internal materials from OFAC regarding the defendant and his presentation at the DPRK Conference; (2) the identity of "Witness-2"; and (3) materials related to the DPRK's cryptocurrency capabilities from various government agencies.

As defense counsel states, the parties have met and conferred in good faith. (Mot. to Compel at 1). The Government voluntarily agreed to several defense requests, without conceding that the requests were within the scope of the Government's discovery obligations, and the parties were therefore able to resolve most discovery disputes. The Government respectfully submits that the three requests in this motion, however, should be denied.

A. The Request for Internal OFAC Documents Should Be Denied

The defendant's first request is for the prosecution team to review and produce OFAC's internal documents and communications. (Mot. to Compel at 7). Because OFAC is not part of the prosecution team, and because the materials sought are not in the prosecution team's possession, custody, or control, this request should be denied.

1. Relevant Facts

On July 29, 2020, the government produced to the defendant records reflecting correspondence between and among the SDNY prosecutors, DOJ's National Security Division ("NSD"), and OFAC. At the defendant's request, the Government also asked OFAC if it would voluntarily provide its internal documents and communications, which were not in the prosecution

---

specific co-conspirator statements the Government may seek to introduce—sufficiently in advance of trial.

team's possession.[10] OFAC, however, informed the prosecutors on September 25, 2020 that it was not able to commit to a voluntary production of documents, and the prosecutors informed the defense.

As reflected in the communications produced by the Government, the first contact between the SDNY prosecutors and OFAC in this case occurred on November 18, 2019, when an attorney assigned to the unit that reviews IEEPA violations for NSD contacted OFAC, and stated: "We have a scenario we'd like to run by someone at OFAC related to a DPRK service. Any chance one of you is available in the next couple of hours?" (USAO_001750). That same day, a member of the prosecution team learned from another NSD lawyer that an OFAC official had asked whether Griffith's presentation fell into the exception for "information or informational materials," *see supra* (the Berman Amendment). (USAO_001744). The NSD lawyer asked: "Do we know how much of the presentation he gave was specifically created for this event vs. a general presentation that he gives otherwise. OFAC says that this is a grey area and general presentations that are given other places may fall under an exception and not require a license, while a specifically created presentation would be a service." (USAO_001745). The prosecutors, NSD, and OFAC spoke by phone that same day at around 2:30 p.m.

The next morning, on November 19, 2019, the NSD lawyer sent an email memo to OFAC, formally requesting "an OFAC Licensing Determination in the matter of Virgil Griffith." (USAO_001746). The memo provided OFAC with a summary of the relevant facts,[11] and an

[10] The prosecution team also asked the U.S. State Department to provide internal documents and communications. They agreed to provide these materials, and on October 30, 2020, the Government produced the responsive materials to the defense.

[11] The prosecution team did not obtain the audio recordings of the Conference and the defendant's remarks until after Griffith was charged by Complaint. Accordingly, the evidence that Griffith's presentation was not fully created and in existence before the Conference has grown stronger since the Griffith was charged.

analysis of why Griffith's presentation did not fall within the exemption for "informational materials." Relevant here, the memo assessed that Griffith's presentation, based on what was known at the time, did not fall under the exemption, "because Griffith created the presentation for the cryptocurrency conference and the DPRK government." (USAO_001747). Additionally, Griffith took questions during the Conference, "during which, by his own admission, Griffith discussed with more knowledgeable conference attendees topics such as the creation of cryptocurrency through mining." (*Id.*). Because Griffith "used his expertise to take publically available information and package it so that the DPRK audience could better understand the concepts and apply it to circumstances that were unique to issues present in particular within the DPRK," the memo assessed that Griffith's conduct violated IEEPA. (*Id.*).

On November 20, 2019, the prosecutors, NSD, and OFAC had another phone call at approximately 2 p.m., during which OFAC stated that it would "get us an answer promptly, and signaled that they would support the prosecution." (USAO_001751). Later that day, OFAC counsel sent an email to the prosecutors and NSD, in which he stated: "I expect we'll be able to get back to you tomorrow (hopefully by noon) with the assurance you need, at least as to Griffith's presentation at the conference. On the facts presented, OFAC may not be comfortable giving the assurance with respect to Griffith's travel to [the DPRK]." (USAO_001754).

On November 21, 2019, around 1:33 p.m., counsel for OFAC sent the prosecutors and NSD an email, which stated:

> This confirms that if asked, OFAC will provide a witness to testify that the facts set out in the attached Sealed Complaint show violations of the North Korea Sanctions Regulations, 31 CFR Part 510. The witness would testify that the presentation by Virgil Griffith at the Cryptocurrency Conference in North Korea referenced in the Sealed Complaint constituted a violation of 31 CFR §§ 510.206(a) (prohibited exportation of services to North Korea) and 510.212(b) (conspiracy to violate prohibitions set forth in 31 CFR Part 510).

> The witness would also testify that on November 15, 2019, OFAC conducted a License History Check to determine whether its records indicate that Mr. Griffith ever sought or obtained a license from OFAC to participate in the Cryptocurrency Conference. The witness would testify that the search disclosed no responsive records of applications submitted by or on behalf of, and no OFAC licenses issued to, any party by the name of Virgil Griffith. See the attached License History Check.

(USAO_001752).

2. Legal Standards

The prosecution team's disclosure obligations extend to material that is in the possession of an entity that has acted as "an 'arm of the prosecutor'" in a given case. *United States v. Blaszczak*, 308 F. Supp. 3d 736, 741 (S.D.N.Y. 2018) (quoting *United States v. Morell*, 524 F.2d 550, 555 (2d Cir. 1975)). Therefore, when the prosecution "'conducts a joint investigation with another state or federal agency, courts in this Circuit have held that the prosecutor's duty extends to reviewing the materials in the possession of that other agency for *Brady* evidence.'" *United States v. Middendorf*, 18 Cr. 36 (JPO), 2018 WL 3956494, at *4 (S.D.N.Y. Aug. 17, 2018) (quoting *United States v. Gupta*, 848 F. Supp. 2d 491, 493 (S.D.N.Y. 2012)).

"A number of factors are relevant in determining whether the prosecution conducted a 'joint investigation'" with another agency. *Middendorf*, 2018 WL 3956494, at *4. The factors include "whether the other agency: (1) participated in the prosecution's witness interviews, (2) was involved in presenting the case to the grand jury, (3) reviewed documents gathered by or shared documents with the prosecution, (4) played a role in the development of prosecutorial strategy, or (5) accompanied the prosecution to court proceedings." *Id.* (citing *Blaszczak*, 308 F. Supp. 3d at 741-42).

In *Middendorf*, the Government and the SEC conducted joint witness interviews and charged the same group of defendants on the same day. Judge Oetken nonetheless found that the Government and the SEC had not conducted a joint investigation, because the SEC was not

involved in the grand jury presentation, had not reviewed documents gathered by the Government or shared the fruits of its investigation with the Government, and did not participate in the overall development of prosecutorial strategy. *Id.* at *5. Judge Kaplan reached a similar conclusion in *Blaszczak*, reasoning that, notwithstanding that the SEC had "furnished documents it collected to the USAO, that the SEC and the USAO interviewed a number of witnesses at the same time, and that the SEC and USAO ultimately informed one another of the enforcement actions each intended to take," the SEC was not an arm of the prosecution because it was not involved in the grand jury presentation, did not review documents gathered only by the prosecution, did not develop prosecutorial strategy, and did not accompany the prosecution team to court proceedings in the SDNY case. *Blaszczak*, 308 F. Supp. 3d at 741.

By contrast, Judge Gardephe in *Martoma* concluded that the Government's *Brady* and *Giglio* obligations extended to communications between the SEC and counsel for two witnesses that were in the sole possession of the SEC, because the Government and SEC had conducted a joint investigation. *United States v. Martoma*, 990 F. Supp. 2d 458, 460 (S.D.N.Y. 2014). There, the court held that the SEC and the Government had been "engaged in joint fact-gathering," because the Government and the SEC had "jointly conducted twenty interviews of twelve," the SEC had provided the Government with documents that it obtained during its investigation, and the SEC and Government coordinated their efforts in conducting depositions. *Id.* at 461. Similarly, Judge Rakoff found a joint investigation in *Gupta*, relying principally on the facts that the Government and the SEC "jointly interviewed no fewer than 44 witnesses," that the SEC attorney had, "within a day or two of each interview, prepared memoranda that summarized what he felt were the relevant parts of the interviews," and that the agencies were thus "engaged in joint fact-gathering." *Gupta*, 848 F. Supp. 2d at 493-94.

3. Discussion

The defendant asserts that the Government must acquire and produce OFAC's internal communications because the Government's pre-charging consultation with OFAC rendered it part of the prosecution team. He is wrong.

As an initial matter, the defendant does not even attempt to address three of the *Middendorf* factors which plainly cannot weigh in his favor: OFAC did not participate in witness interviews, present the case to the grand jury, or accompany the prosecution to court proceedings. *See Middendorf*, 2018 WL 3956494 at *4. These three out of five factors already counsel against finding OFAC a member of the prosecution team.

To the extent OFAC reviewed information gathered by the Government or played any role in the development of prosecutorial strategy, it did so in its capacity as experts independently responsible for administering the NKSR. For example, the communications raised by the defense and summarized above reflected efforts by the prosecutors to (1) ensure that OFAC agreed with the prosecutors' legal assessment of evidence that the prosecutors and agents had collected—without OFAC—with respect to the application of the sanctions program that OFAC administers, and (2) secure an expert witness from OFAC to testify at a trial that the prosecutors, NSD, and FBI had already started to plan for at the time of the communications. As an independent agency, OFAC routinely renders determinations regarding the regulations it administers. As discussed *supra*, those determinations are often entitled to deference. The communications reveal OFAC's involvement was consistent with that role, and more akin to a consulting expert or expert witness—a role in which an OFAC representative will ultimately serve.

OFAC's review of information gathered by the Government here occurred only after the initial, pre-charging investigation had been largely completed. In fact, the communications cited by Griffith between OFAC and the prosecutors show that OFAC, at least initially, knew little about

the facts of the case and asked for information to better assess whether the defendant's presentation fell within the Berman Amendment's exemption for informational materials. After receiving more information about the facts, OFAC determined that it could provide a witness for trial who would testify that Griffith's presentation was, under the NKSR, a prohibited exportation of services to the DPRK, and that no license had been granted to permit Griffith to do so. (USAO_001752). OFAC has not played a role in executing search warrants or similar fact-gathering tasks specific to this investigation. Its review of information gathered by the Government to date has been limited to the purposes set forth above, as corroborated by the cited communications.

OFAC was consulted prior to charging this case and reviewed a draft complaint, playing a discrete role in the development of prosecutorial strategy. However, this consultation does not render OFAC a member of the prosecution team, even if OFAC's input affected the prosecutorial strategy. In *United States v. Stewart*, 433 F.3d 273, 298 (2d Cir. 2006), the Second Circuit considered whether a Secret Service employee who testified as an expert in "ink" was a member of the prosecution team. In upholding the district court's conclusion that the expert was not, the Court explained that the expert was not "in any way involved with the investigation or presentation of the case to the grand jury," and "did not interview witnesses or gather facts." *Id*. at 298-99. The Court noted that the expert reviewed the evidence about which he testified and likely altered the prosecutorial strategy through his expertise. *Id*. Nonetheless, the Court found the witness acted "only in the capacity of an expert witness, as the District Court found, and not as a 'fully functioning member of the prosecution team.'" *Id*. For the same reasons, the consultation with OFAC on which Griffith concentrates did not turn OFAC from an expert in the regulations into a full-fledged member of the prosecution team.

OFAC's limited role in this case does not transform OFAC into an arm of the prosecution, such that the prosecution team is required (or able) to obtain OFAC's internal communications. As explained above, the Government has asked OFAC to voluntarily provide the prosecution team with their internal documents and communications, and OFAC declined.

The out-of-Circuit cases cited by the defendant are readily distinguishable. In *United States v. Wood*, 57 F.3d 733, 737 (9th Cir. 1995), two defendants were charged with a conspiracy to defraud the FDA by obstructing the FDA's function of ensuring that prescription drugs are safe, effective, and dispensed pursuant to a prescription from a practitioner licensed by law to administer such drugs. 57 F.3d at 735. In that case, the FDA "s[ought] the prosecution" of the defendant, and the district court had directed the Government, before trial, to provide to the defendant "all information falling within Rule 16, including information in the custody of the FDA, forthwith." *Id.* at 736 (internal quotation marks omitted). Accordingly, there was no dispute in that case that the FDA and U.S. Attorney's Office had conducted a joint investigation. *United States v. Walker*, 746 F.3d 300, 306 (7th Cir. 2014) and *United States v. Zuno-Arce*, 44 F.3d 1420, 1427 (9th Cir. 1995) stand for the uncontroversial proposition that the Government's disclosure obligations extend to other members of the prosecution team. Finally, the defense cites to *United States v. Brooks*, 966 F.2d 1500, 1504 (D.C. Cir 1992) to support its claim that the Government should be required to search agencies who were "involved in the underlying charged conduct at issue" as well as "the investigation." (Mot. to Compel at 11). That out-of-Circuit case, however, does not change the fact that "[i]n the Second Circuit, a prosecutor's constructive knowledge only extends to those individuals who are 'an arm of the prosecutor' or part of the 'prosecution team.'" *United States v. Meregildo*, 920 F. Supp. 2d 434, 440–41 (S.D.N.Y. 2013), *aff'd sub nom. United States v. Pierce*, 785 F.3d 832 (2d Cir. 2015) (quoting *United States v. Gil*, 297 F.3d 93, 106 (2d Cir.

2002)). Nonetheless, in contrast to *Brooks*, where the law enforcement agency at issue had a "close working relationship between the Washington metropolitan police and the U.S. Attorney for the District of Columbia (who prosecutes both federal and District crimes, in both the federal and Superior courts), a relationship obviously at work in this prosecution," the communications cited by the defendant demonstrate that OFAC was consulted on discrete matters in its capacity as administrators and experts for the NKSR. *Brooks*, 966 F.2d at 1503.

Because the *Middendorf* factors counsel against a finding that OFAC is member of the prosecution team, the defendant's request that the Court compel OFAC to provide its internal documents should be denied.

B. The Request for Immediate Disclosure of Witness-2's Identity Should be Denied

Griffith next requests the identity of a witness that the Government has identified as Witness-2. But Griffith fails to overcome the general rule that "[n]othing . . . obligates the Government to disclose the identity of its prospective witnesses before trial." *Castellaneta*, 2006 WL 3392761, at *2. As this Court has noted, "[t]he government need not produce and the Court is prohibited from ordering the production of statements by government witnesses 'until said witness has testified on direct examination in the trial of the case.'" *Nigro v. United States*, No. 09-CR-1239 (PKC), 2016 WL 3211968, at *2 (S.D.N.Y. June 9, 2016) (Castel, J.) (quoting 18 U.S.C. § 3500(a)). Indeed, at the initial pretrial conference in this case, on January 30, 2020, counsel for Griffith requested "FBI 302s or whatever interviews they've done of [other people who attended the Conference] as soon possible . . . ." (ECF No. 25 at 7). In response, the Court stated, "I don't understand the basis for your getting statements by people who the government may or may not elect to call as witnesses unless the statements are exculpatory to your client, in which event the government has an obligation to produce them under *Brady*." (*Id.*).

Nonetheless, the Government has provided the defense with witness statements, emails, and law enforcement reports that constitute Jenks Act materials for 10 total witnesses, including individuals living abroad and law enforcement witnesses. As to Witness-2, the Government has provided the defense with: (1) a redacted FBI report reflecting the FBI's interview of Witness-2; (2) a redacted report reflecting Witness-2's proffer with the Government; (3) communications provided by Witness-2 with other Conference participants; (4) photographs of the Conference provided by Witness-2; and (5) audio recordings of the Conference made by Witness-2. The Government also informed the defense that: (1) Witness-2 resides abroad; (2) the recordings provided by Witness-2 were not made at the Government's request; (3) that the Government plans to call Witness-2 at trial; and (4) that Witness-2 is represented by counsel. The Government also provided the defense with Witness-2's counsel's name and contact information. Finally, the Government informed defense counsel that it intends to disclose the name of Witness-2, as well as unredacted witness statements, 30 days before trial. These disclosures far exceed the Government's obligations under the Jencks Act at this stage of the prosecution. *See Nigro*, 2016 WL 3211968, at *2 (noting custom of producing 3500 material "the Thursday before the start of a Monday trial"); *Castellaneta*, 2006 WL 3392761, at *2.

Moreover, although there is no legal obligation on the part of the Government to provide a witness's name, and the Government is not required to identify to the defense a "specific or cognizable threat to the safety of Witness-2," (Mot. to Compel at 13), there are reasons to believe that Witness-2's ability to work and his safety might be negatively affected if his identity is disclosed. In particular, the Government has learned that individuals supportive of the defendant are seeking to identify any individuals assisting the Government, potentially, for the purpose of applying pressure to prospective Government witnesses or to deter cooperation with the

investigation.[12] In addition, the DPRK has a long and detailed public history of violence against those opposed to the regime.[13] Even if a protective order could mitigate these concerns, it will not eliminate these risks. These issues only compound the reasons why disclosure of Witness-2's identity is not necessary or proper at this stage of the case.

Despite these risks, the defense seeks an order compelling production of Witness-2's identity. The Court "may compel pretrial disclosure of the identity of government witnesses on a 'specific showing' that such disclosure is both material to the defense and reasonable in light of the circumstances of the case." *Delacruz*, 2015 WL 2211943, at *3 (quoting *United States v. Bejasa*, 904 F.2d 137, 139–40 (2d Cir. 1990) (emphasis in original)). However, the defendant has made no such specific showing here.

The defendant first argues that the facts regarding the provenance of the recording, its authenticity, and its chain of custody are material to the preparation of the defense. (Mot. to Compel at 12). The defense is free to inquire of Witness-2's counsel regarding these details and to examine the recordings themselves, and does not need to know Witness-2's identity in order to do so or further investigate these issues now.

The defense next claims that they need to know Witness-2's identity so they can consider a motion to depose Witness-2 under Federal Rule of Criminal Procedure 15. (Mot. to Compel at 13). But there is no reason why the defense needs to know the witness's identity in order to bring such a motion. Rule 15 permits a motion to take a deposition on notice and "because of exceptional circumstances." Fed. R. Crim. P. 15(a)(1). The Second Circuit has held that "exceptional

[12] As noted by the defendant, based on the currently available information, the Government does not assert that the defendant is involved in these efforts.

[13] Robert Windrem, et al., "North Korea has a history of assassination attempts on foreign soil," *NBC News* (Nov. 21, 2017), Available: https://www.nbcnews.com/news/north-korea/north-korea-has-history-assassination-attempts-foreign-soil-n823016

circumstances" exist where the moving party can "show that (1) the prospective witness is unavailable for trial, (2) the witness' testimony is material, and (3) the testimony is necessary to prevent a failure of justice." *United States v. Cohen*, 260 F.3d 68, 78 (2d Cir. 2001); *see also United States v. Spencer*, 362 F. App'x 163, 164 (2d Cir. 2010).

The defendant has sufficient information to file a motion for a Rule 15 deposition. The defense is aware that Witness-2 lives abroad and is therefore not subject to the Government's subpoena power. The Government has told the defense that it intends to seek Witness-2's testimony, but that it cannot guarantee that Witness-2 will voluntarily appear in court to testify and cannot compel Witness-2 to do so. The disclosure of Witness-2's statements provides the defense with notice regarding the nature of Witness-2's anticipated testimony, as does the disclosure of the recordings themselves. The defense does not explain how learning the witness's identity would change the calculus on seeking a Rule 15 deposition.

For all these reasons, the defendant's motion for immediate disclosure of Witness-2's identity should be denied.

C. Documents and Communications Related to the DPRK's Cryptocurrency and Blockchain Capabilities Are Not Discoverable

Finally, Griffith asks the court to compel the Government to produce DOJ, FBI, OFAC, Central Intelligence Agency, and National Security Agency documents and communications related to the DPRK's cryptocurrency and blockchain capabilities. (Mot. to Compel at 14-15). The Government has agreed to search the FBI's files related to this case for this information, and to provide unclassified responsive documents to the defense. However, the Government respectfully submits that a wide-ranging and open-ended search of the files of five different agencies—two from the intelligence community—is unduly burdensome and reaches far beyond the possession, custody, or control of the prosecution team. *See United States v. Avellino*, 136

F.3d 249, 255-56 (2d Cir. 1998) ("[T]he imposition of an unlimited duty on a prosecutor to inquire of other offices not working with the prosecutor's office on the case in question would inappropriately require us to adopt a monolithic view of government that would condemn the prosecution of criminal cases to a state of paralysis." (internal quotation marks and citation omitted)); *see also United States v. Locascio*, 6 F.3d 924, 949 (2d Cir. 1993), *cert. denied*, 511 U.S. 1070 (1994) (refusing to impute to prosecutors knowledge of FBI reports prepared by agents "uninvolved in the investigation or trial" of defendants); *United States v. Quinn*, 445 F.2d 940, 944 (2d Cir.), *cert. denied*, 404 U.S. 850 (1971) (rejecting as "completely untenable the position that knowledge of any part of the government is equivalent to knowledge on the part of this prosecutor" (internal quotation marks and alternations omitted))).

Moreover, because the information sought does not bear on the elements of the offense charged, the defense has also failed to establish that it is entitled to the information it seeks. In support of his motion, Griffith asserts that "one of the 'services' the government alleges that Mr. Griffith provided to the DPRK was the provision of information that it did not otherwise have regarding blockchain technology and cryptocurrency." (Mot. to Compel at 14). This is not accurate. The Government has not alleged, and need not prove at trial, that the Griffith's remarks imparted wholly unknown information in order to constitute services under the NKSR. To convict Griffith on the sole count of the Indictment, the Government must only prove that the defendant willfully agreed to provide services to the DPRK or to evade and avoid sanctions against the DPRK, or attempt to do so, with the intent that the conspiracy succeed.

It is not material what the DPRK knew or did not know about blockchain and cryptocurrency technologies, let alone what United States intelligence agencies understood about what the DPRK knew or did not know. What matters is that Griffith conspired to provide the

DPRK, and individuals living in North Korea, with a service, and to evade and avoid U.S. sanctions against the DPRK. *See Banki*, 685 F.3d at 108 (stating that the Iranian sanctions "prohibit the exportation of not only advice on developing Iranian chemical weapons but also advice on developing Iranian petroleum resources, *see* § 560.209; not only services to the Iranian government but also services to Iranian businesses, *see* § 560.204; and not only bombs but also beer, *see* § 560.204"). As explained in detail above, Griffith provided a service to the DPRK and the North Korean Conference attendees by synthesizing information about blockchain and cryptocurrency, explaining how North Koreans could use those technologies to evade sanctions, and answering follow-up questions from the North Korean citizens and government officials in attendance at the Conference.

Finally, the inchoate nature of the charged offense further underscores the irrelevance of the information sought by the defense. The Government need not prove that Griffith's services were helpful to any individual attending the conference so long as Griffith agreed with others and *intended* to provide a service, to evade or avoid sanctions, or attempt to do so. The conspiracy need not have succeeded in providing the DPRK with a service, let alone one that was demonstrably helpful to the DPRK. The information Griffith demands that the prosecution team seek on his behalf has no bearing Griffith's intent—he had no way of truly knowing what the DPRK or the individual conference attendees knew about blockchain and cryptocurrency technologies, and the defense does not claim otherwise. The defendant's self-serving—and irrelevant—claim that he did not believe his presentation would be helpful to anyone at the Conference is belied by the defendant's remarks at the Conference and his admissions to the FBI. As Griffith told the FBI, he believed that he introduced new concepts to the North Korean Conference attendees, and that the attendees left with a better understanding of blockchain and

cryptocurrency technologies. And as Griffith told the Conference attendees, "the technology is still fairly new . . . [s]o . . . no one knows how to do all this right yet, but we definitely think this will be really useful for the DPRK, and that's why we're here. And if the DPRK adopts this, they will be on the very leading edge of technology." (USAO_002622).

Because the information sought by the defendant is not material to a defense in this case, and because the request exceeds the scope of the Government's obligations under Rule 16, *Brady*, and *Giglio*, the defendant's request for documents and communications related to the DPRK's cryptocurrency and blockchain capabilities from the DOJ, FBI, OFAC, Central Intelligence Agency, and National Security Agency should be denied.

CONCLUSION

For the foregoing reasons, the Government respectfully requests that the Court deny the defendant's motions to dismiss the Indictment, for a bill of particulars, and to compel discovery in their entirety.

DATED: New York, New York
November 19, 2020

Respectfully submitted,

AUDREY STRAUSS
Acting United States Attorney
Southern District of New York

By: /s/
Michael Krouse
Kimberly J. Ravener
Kyle Wirshba
Assistant United States Attorneys
Tel: (212) 637-2279/2358/2493